US005442701A

United States Patent [19]

Guillou et al.

[11] Patent Number: 5,442,701

[45] Date of Patent: Aug. 15, 1995

[54] **PROCESS FOR THE BROADCASTING OF CONDITIONAL ACCESS PROGRAMS PERMITTING A PROGRESSIVE ACCESS TO SUCH PROGRAMS**

[75] Inventors: **Louis Guillou**, Bourgbarre; **Jean-Luc Giachetti**, Rennes; **Alain Gelly**, Paris, all of France

[73] Assignees: **France Telecom Etablissement Autonome de Droit Public**; **Telediffusion de France S.A.**, both of Paris, France

[21] Appl. No.: **172,817**

[22] Filed: **Dec. 27, 1993**

[30] **Foreign Application Priority Data**

Dec. 29, 1992 [FR] France 92 15841

[51] **Int. Cl.**[6] **H04N 7/167**

[52] **U.S. Cl.** **380/20**; 380/10; 380/19

[58] **Field of Search** 380/9, 10, 20, 19

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,994,909 2/1991 Graves et al. 358/86

Primary Examiner—David C. Cain

Attorney, Agent, or Firm—Oblon, Spivak, McClelland, Maier, & Neustadt

[57] **ABSTRACT**

A process for broadcasting conditional access programs which permits a progressive access. Scrambled program data is transmitted along with partial access checking messages and complete access checking messages such that subscribers having a partial access right may descramble portions of the scrambled data corresponding to information regarding only the identity of the conditional access programs, and subscribers having a complete access right may descramble the remainder of the scrambled data and view the conditional access programs. The conditional access programs may be television pictures, radio programs, or data broadcasts.

9 Claims, No Drawings

PROCESS FOR THE BROADCASTING OF CONDITIONAL ACCESS PROGRAMS PERMITTING A PROGRESSIVE ACCESS TO SUCH PROGRAMS

FIELD OF THE INVENTION

The present invention relates to a process for the broadcasting of conditional access programs permitting a progressive access, as well as to a process for the progressive access to such programs.

This invention is used in pay television, in the broadcasting of radio programs or sound or data, in the transmission and distribution of program elements intended to be integrated into the programs of program companies or cable distributors, within the framework of satellite reporting exchanges, e.g. in the news, sport or entertainments fields.

DESCRIPTION OF THE PRIOR ART

In conventional systems, access to programs is reserved for a certain population of receivers. A distinction can be made between various access rights (e.g. a program can be simultaneously accessible by subscription and by impulse buying), so that a receiver is authorized or not as a function of whether it does or does not have a certain access right.

This state of affairs does not enable a televiewer to decide, in the possession of all necessary information, what his interest would be in having access to a particular program. Conversely, for the organization offering programs, there are no direct means for inciting the televiewer to acquire new access rights except by indirectly supplying him by advertising or personalized mail with information relative to all available programs.

SUMMARY OF THE INVENTION

The present invention aims at obviating this disadvantage. To this end it proposes a process which gives a summary of certain programs. This summary is made possible by the use of an only partial access right, as opposed to the normal and total access right. Thus, in addition to authorized receivers who can have complete access to a program and unauthorized receivers who can receive nothing of such a program, according to the invention there are other receivers which could have a summary of the program, i.e. access to a discernible, but unusable form of the program.

This partial access right introduced by the invention will be referred to as "summary right" in the remainder of the description. Receivers having such a summary right will be referred to as "restricted receivers".

Thus, with the invention, there are no longer two, but instead generally three perception levels, namely the case where the picture is clear, the case where the picture is discernible, but not usable and the case where the picture is no longer discernible.

Users of restricted receivers could then choose to acquire an access right for a particular program with complete knowledge thereof. Therefore there is an incitement aspect.

For example, the process according to the invention can advantageously be applied to:

- incitement to subscribing to pay television,
- incitement to impulse consumption of pay television programs,
- incitement to purchase programs proposed by owners of rights, program companies or producers, within the framework of program exchanges or reports by satellite, e.g. in the news, sport or entertainments fields.

More specifically, the present invention relates to a process for broadcasting conditional access programs, in which in known manner:

- informations specific to various programs are scrambled,
- the thus scrambled informations are transmitted for each program,
- synchronized with each program transmission takes place of access checking messages specific to each of these programs and which are able to permit the descrambling and restoration of programs in receivers having corresponding access rights,

said process being characterized in that there is also a transmission of partial access checking messages to at least some of these programs, said partial access checking messages being able to permit the descrambling and partial restoration of the corresponding programs for receivers having a partial access right.

Advantageously, to permit the performance of this process the information flow corresponding to each program is subdivided into a first or elementary flow corresponding to a program which, once restored in a receiver, will be discernible without being directly usable, and a second or complementary flow making it possible to complete the first flow, so as to permit the complete restoration of the program.

In this variant, the partial access checking messages will apply to the elementary flows.

The present invention also relates to a process for progressive access to programs, which have been transmitted in the manner described hereinbefore. In this process and in per se known manner:

- selection takes place of a program and an access checking message relative to said selected program is received, scrambled informations are received,
- with the aid of the message and an access right, the selected program informations are descrambled,

characterized in that:

- partial access checking messages are also received,
- by means of a partial access right, descrambling and partial restoration of the corresponding program take place,
- optionally, there is an acquisition of an access right in order to have complete access to said program.

The definition given hereinbefore of the invention with transmission of partial access checking messages and partial restoration of a program with the aid of a partial access right, is not limited to the sole case where the picture corresponding to the partial access right is a summary of a picture, i.e. a perceptible, but unusable picture. This definition also covers the case where the picture obtained has a quality below that of a picture which would use all the broadcast information, but which would still be usable. The different receivers utilizing the invention can therefore have different perception levels. Certain receivers could operate with a very high picture quality level and for this purpose would have to use all the transmitted information (if provided with the corresponding access right). However, other receivers would operate with a lower quality level, but which would still be acceptable and involving only part of the transmitted informations (if they are provided with a partial access right).

For example, a high definition television program HDMAC can be received by D2MAC receivers. In this situation, it would be desirable that D2MAC receivers would be less "indebted" than HDMAC receivers. Such a result is possible with the invention with the following perception levels:

completely scrambled program,

D2MAC perception,

HDMAC perception.

It is naturally also possible to introduce in the above hierarchy, a restricted perception level leading to perceptible, but unusable pictures, in order to incite the televiewer to acquire access rights corresponding to a higher perception level in the hierarchy.

However, in the following description and for simplification purposes, there will be a limitation to the case where introduction occurs of a partial access right corresponding to discernible, but unusable pictures.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The process according to the invention can be implemented in advantageous manner by organizing a video component in at least two flows, when it is a question of transmitting television programs. A first or elementary flow makes it possible to obtain a discernible picture, which is not directly usable. A second or complementary flow makes it possible to obtain the remainder of the video component.

At least three methods make it possible to bring about such a subdivision of the video component. This subdivision can be quality, space or time based.

a) In a quality subdivision, the elementary flow transports all the informations giving a very mediocre quality picture. The complementary flow transports the informations giving the picture its full quality. Quality subdivision can also be looked upon as an extension of hierarchic coding, which makes it possible to obtain different perception levels with the same signal. With the presently indexed quality levels (VHS equivalent quality, SECAM equivalent quality, D2MAC equivalent quality and HD equivalent quality) is added a very mediocre quality level supplying a discernible, but unusable picture.

b) In a space subdivision, the picture is e.g. subdivided horizontally into a few bands of a few consecutive lines. One part of the bands (e.g. half) constitutes the elementary flow and the other part (the other half), constitutes the complementary flow.

c) In a time subdivision, the time is broken down into periods of a certain duration (e.g. about ten seconds). Part of the period (2 to 3 seconds) constitutes the elementary flow, whereas the remainder of the period constitutes the complementary flow.

In this case, it is the very principle of time subdivision at a sufficiently high frequency which makes it possible to obtain a discernible, but not directly usable program.

No matter which variant is chosen, the process according to the invention consists firstly of separately scrambling each of the flows, e.g. with sequences of different check words and then allocating access criteria to each sequence of check words, so that the following conditions are satisfied:

- an access right permits access to two sequences of check words,
- a partial right or summary permits access only to the sequence of check words permitting the descrambling of the elementary flow.

Thus, the holder of a summary right can discern the presence of a program and can even evaluate its nature and interest. If he wishes, he can then acquire an access right so as to give access to the complete program.

In the preceding variant, the two flows are scrambled by two series of different words. In another variant, it is possible to use a same series of check words for scrambling the two flows. Thus, knowing that the check words have a limited life (approximately 10 seconds in D2MAC Eurocrypt), it is possible to define three populations of receivers, namely receivers not having the check word do not see the program, receivers having the check word in uncoded form throughout its validity period have access to the program and receivers having access to check words during the final instance of their validity period have access to the summary.

This latter case is possible by adding to the access control message system a few seconds prior to the end of the life of each check word, a new criterion, which is constituted by the summary criterion, authorizing access to the check word finishing its life. This new criterion will be used by restricted receivers. Obviously, during the life of a check word, the following check word cryptogram must not be broadcast.

The following diagrams illustrate this variant in the case where each check word has a life of 10 sec. In this case the abbreviation AC stands for the access criterion, AP for the summary criterion, CWe (or CW'e) for the cryptogram of an even check word and CWo (or CW'o) the cryptogram for an uneven check word.

The messages transmitted are then as follows, during the different periods:

first period: AC (CWo, CWe) during 7 seconds,
then AC, AP (CWe) for 3 seconds,
second period AC, (CWo, CW'e) for 7 seconds,
then AC, AP (CWo) for 3 seconds,
third period AC, (CW'o, CW'e) for 7 seconds,
then AC, AP, (CW'e) for 3 seconds.

With such a diagram every ten seconds, for three seconds, the receivers having a summary right are able to reconstitute the program.

If several programs are carried on the same network, all the programs can use the same summary criterion and the same check word for authorizing descrambling of the elementary flow. Thus, if the user has this check word, he will rapidly acquire access to the elementary flows of all the programs of the network without having to acquire or calculate a new right and a new check word for each program. This implementation makes it possible to eliminate the switching time due to the conditional access on passing from one program to another within a group of programs, whose scrambling is synchronized at the transmission point.

It must be stressed that the invention is particularly advantageous when the transmitted signals are of a digital nature (as opposed to analog signals). It is pointed out in this connection that the scrambling procedures give rise to two contradictory constraints:

- on the one hand, the comfort of the user, which must not be impaired by the scrambling, so that the scrambling methods must not increase the errors or distortions introduced by faults due to transmission, this applying between scrambling operations centralized at the transmission point and descrambling operations performed in each decoder;
- on the other hand piracy, which must be made difficult, so that the signal must be well protected.

In practice, scrambling must be adapted to the encoding of each component of the service: pictures, sound and data. Thus, the possible processing operations on analog elements of the signal remain very limited, because when the operations become complicated, deteriorations due to the successive scrambling and descrambling operations rapidly become unacceptable for users. In other words, the hitherto most widely used standards for the transmission of sound and television pictures (SECAM, PAL and NTSC) are not economically compatible with the processing operations which would make the signal very difficult to pirate. The correlation between the scrambled signal and the signal in uncoded form therefore remains very important. For example, the pictures due to the DISCRET I process presently used by the CANAL PLUS chain remain very recognizable. These pictures can be easily reconstituted by pirates. In order to limit fraud, it is necessary to have sophisticated scrambling methods, which are not very compatible with the objective of obtaining an inexpensive decoder.

The situation is radically modified for digital elements of the signal. There can then be considerable protection, even with a summary scrambling operation consisting of the bitwise combination by an exclusive-OR logic gate of the sequences of bits representing digitized signal samples with sequences of bits produced by a pseudorandom generator. For example, the scrambled pictures received on a 34 Mbit digital television decoder allow nothing to appear. The correlation between the scrambled signal and a signal in uncoded form becomes very difficult. Thus, there can be no incitement. By introducing access to a summary, the process according to the invention makes it possible to obviate this disadvantage.

We claim:

1. A method of broadcasting conditional access programs, comprising the steps of:

(a) scrambling data representing a content of at least conditional access program; and

(b) transmitting such scrambled data along with partial access checking messages and complete access checking messages to subscribers, said partial access checking messages permitting said subscribers to descramble portions of said scrambled data corresponding to information regarding only the identity of said at least one conditional access program, and said complete access checking messages permitting authorized subscribers to descramble a remainder of said scrambled data and view said at least one conditional access program.

2. The method according to claim 1, wherein said at least one conditional access program is a television program, and a video component of television signals is scrambled in step (a) and transmitted in step (b).

3. The method according to claim 2, wherein each television picture to be scrambled is horizontally subdivided into bands of a plurality of consecutive lines, and said scrambled data is derived from a first part of said bands while said partial access checking messages and said complete access checking messages are derived from a second part of said bands.

4. The method according to claim 2, wherein said television signals are subdivided into time periods, and said scrambled data is derived from information present in one part of each time period while said partial access checking messages and said complete access checking messages are derived from information present in a remainder of each of said time periods.

5. The method according to claim 1, wherein said partial access checking messages and said complete access checking messages are separately scrambled using first and second check word sequences, respectively, such that subscribers having a complete access right have access to both said first and second check word sequences, while subscribers having a partial access right only have access to said first check word sequence.

6. The method according to claim 1, wherein said partial access checking messages and said complete access checking messages are scrambled with a single check word sequence having a finite duration, such that subscribers having a complete access right have access to said check word sequence throughout its duration while subscribers having only a partial access right only have access to said check word sequence during a limited portion of its duration.

7. The method according to claim 1, wherein said at least one conditional access program is a television program, and an audio component of television signals is scrambled in step (a) and transmitted in step (b).

8. A method according to claim 1, wherein said at Least one conditional access program is a radio program.

9. A method according to claim 1, wherein said at least one conditional access program is a data broadcasting program.

* * * * *

US005742681A

United States Patent [19]

Giachetti et al.

[11] Patent Number: 5,742,681

[45] Date of Patent: Apr. 21, 1998

[54] **PROCESS FOR THE BROADCASTING OF PROGRAMMES WITH PROGRESSIVE CONDITIONAL ACCESS AND SEPARATION OF THE INFORMATION FLOW AND THE CORRESPONDING RECEIVER**

[75] Inventors: **Jean-Luc Giachetti**, Betton; **Louis Guillou**, Bourgbaré ; **Jean-Claude Pacaud**, Cancale, all of France

[73] Assignees: **France Telecom**; **Telediffusion de France**, both of Paris, France

[21] Appl. No.: **415,987**

[22] Filed: **Apr. 4, 1995**

[30] **Foreign Application Priority Data**

Apr. 6, 1994 [FR] France 94 04012

[51] **Int. Cl.**^{6} **H04N 7/167**

[52] **U.S. Cl.** **380/20**; 380/5; 380/49; 380/10

[58] **Field of Search** 380/20, 23. 4, 380/5, 49

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,349,641 9/1994 Coutrot et al. 380/20
5,517,502 5/1996 Bestler et al. 370/94.2

FOREIGN PATENT DOCUMENTS

0 461 029 12/1991 European Pat. Off. .

0 583 202 2/1994 European Pat. Off. .

OTHER PUBLICATIONS

18th International Television Symposium and Technical Exhibition, Jun. 15, 1993, Montreux, Switzerland, pp. 761–769, may 10, 1993, Jean–Pierre Vigarie, "A Device for Real–Time Modification of Access Conditions in a D2–MAC/Packet Eurocrypt Signal: The Transcontroller".

IEEE Transactions on Consumer Electronics, vol. 38, No. 3, Aug. 1992, pp. 188–194, Didier Angebaud, et al., "Conditional Acess Mechanisms for All–Digital Broadcast Signals".

Primary Examiner—David C. Cain
Attorney, Agent, or Firm—Oblon, Spivak, McClelland, Maier & Neustadt, P.C.

[57] **ABSTRACT**

Process for the broadcasting of programmes with progressive conditional access and separation of the information flow, as well as the corresponding receiver,

In order to form the elementary flow, groups of m successive elements of the multiplex are taken and for forming the complimentary flow groups of p successive elements of the multiplex are taken.

Application to television with entitlement checking.

20 Claims, 4 Drawing Sheets

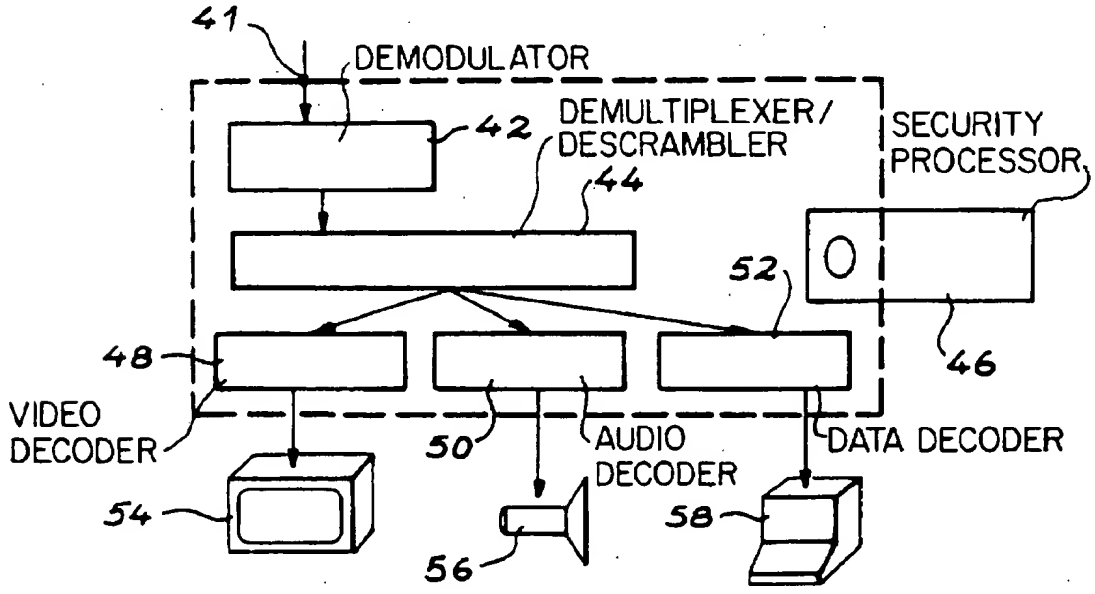


FIG. 1

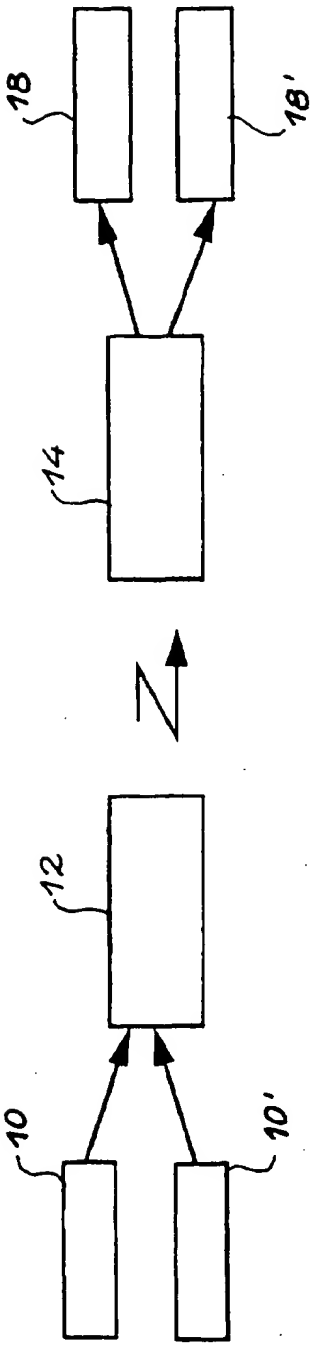


FIG. 2

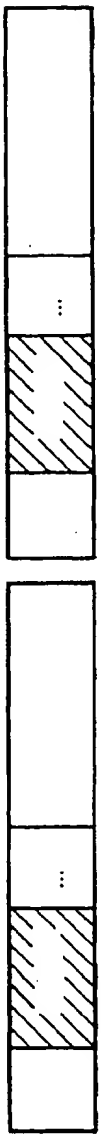


FIG. 3

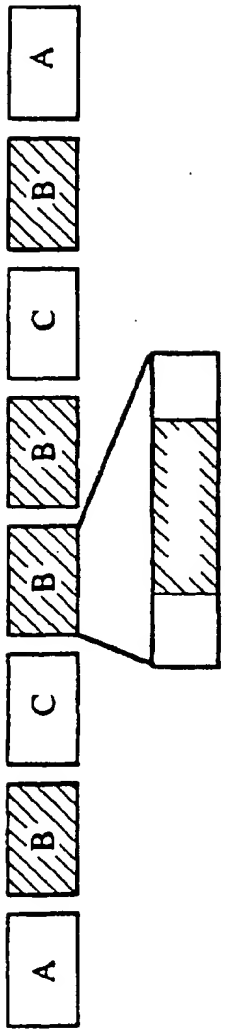


FIG. 4

FIG. 5

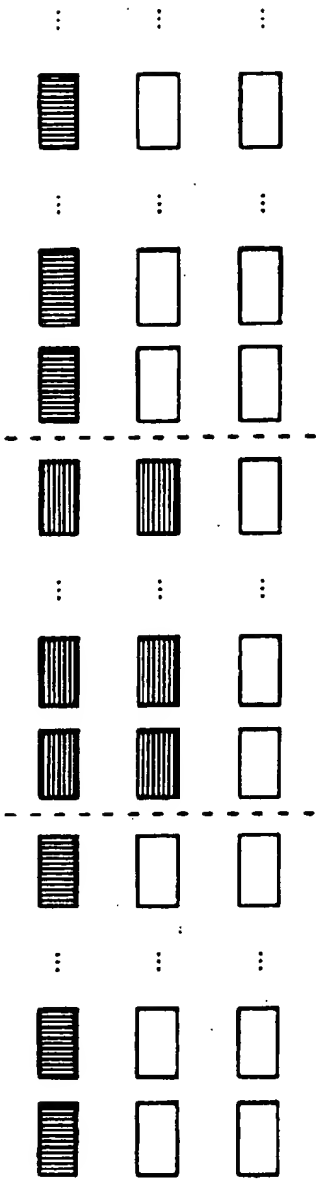


FIG. 6

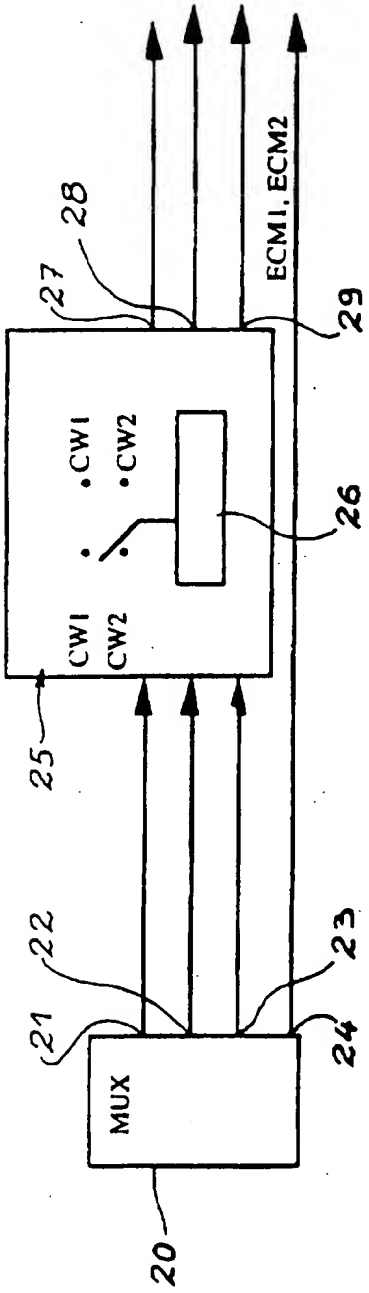


FIG. 7

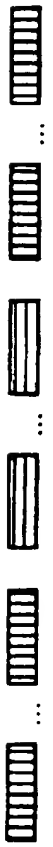


FIG. 8

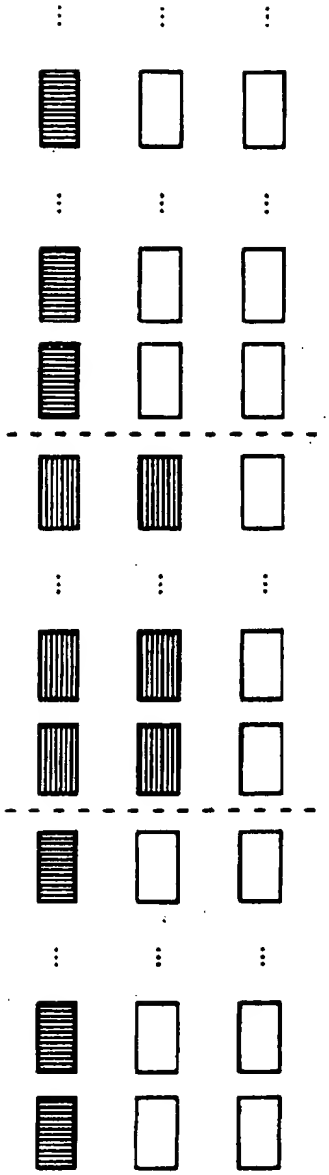
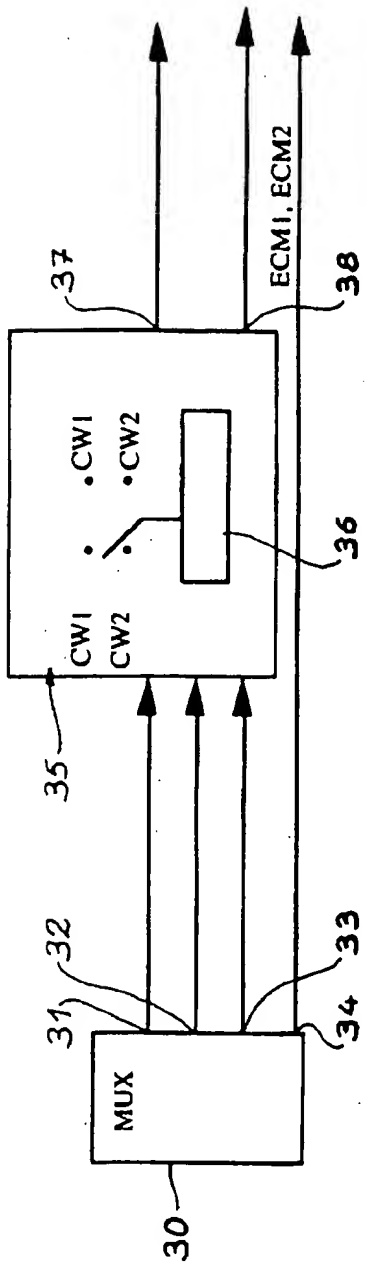


FIG. 9



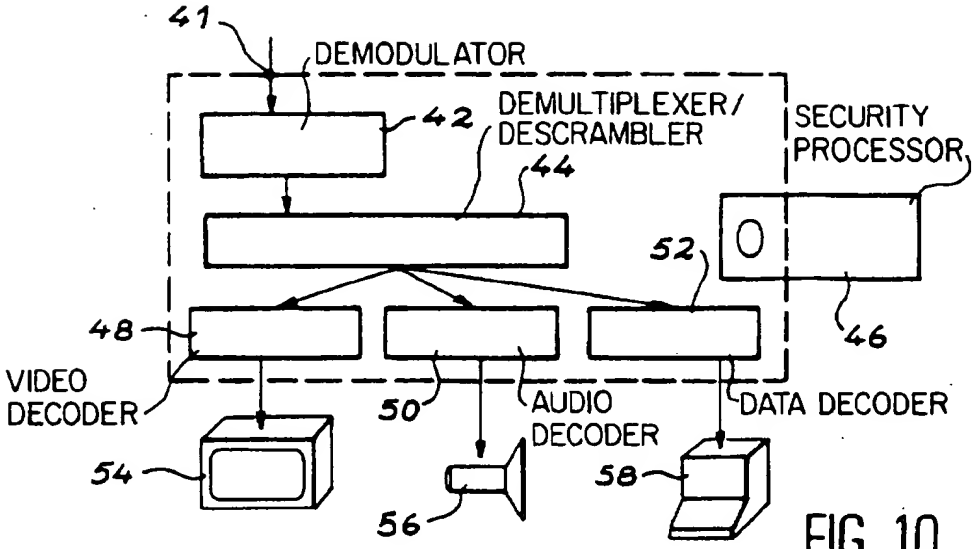


FIG. 10

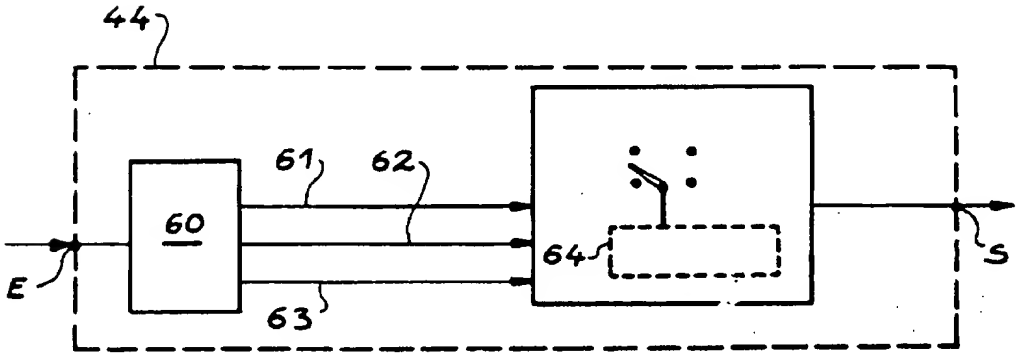


FIG. 11

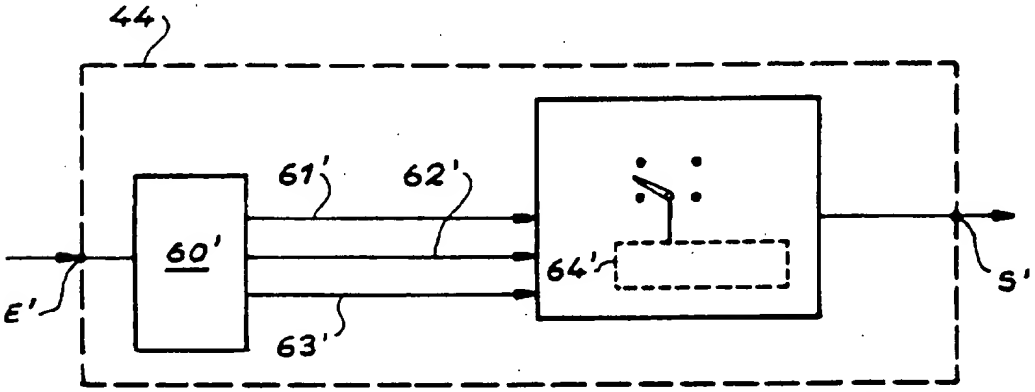


FIG. 12

PROCESS FOR THE BROADCASTING OF PROGRAMMES WITH PROGRESSIVE CONDITIONAL ACCESS AND SEPARATION OF THE INFORMATION FLOW AND THE CORRESPONDING RECEIVER

TECHNICAL FIELD

The present invention relates to a process for the broadcasting of programmes having a progressive access and separation of the information flow, as well as the corresponding receiver.

It is used in pay television, in the broadcasting of radio, sound or data programmes, in the transmission and distribution of programme elements, etc.

PRIOR ART

In conventional programme broadcasting systems, access to the programmes is reserved for a certain population of receivers. Although it is possible to distinguish between different access rights (e,g. a programme can be simultaneously accessible by subscription and impulse buying), it remains that a receiver is or is not authorized as a function of whether it does or does not have a certain access right.

However, the possibility of attracting the television viewer or listener by voluntarily discovering all or part of the content of the picture or sound of a programme during a given time period is an important commercial advantage for any conditional access system. This function exists at present on certain pay television systems using a scrambling process which does not deeply transform the picture. However, digitally, the currently used scrambling methods excessively transform the signal to enable the user to "guess" the programme.

French patent application 92 15841 filed on Dec. 29 1992 and entitled "Process for broadcasting conditional access programmes permitting a progressive access to such programmes" or the corresponding U.S. application Ser. No. 08/172,817 of Dec. 27 1993 describes a method making it possible to have a "glimpse" of certain programmes. This glimpse is made possible by the use of an access right of an only partial nature, unlike in the case of the total, standard access right. Thus, apart from authorized receivers, which can completely access a programme and unauthorized receivers, which cannot receive anything of said programme, according to this procedure, there are other receivers which can have a glimpse of the programme, i.e. being able to access a discernible, but non-usable form of the programme.

The process described in the aforementioned patent application has the following operations:

- informations individual to various programmes are scrambled,
- the thus scrambled informations are transmitted for each programme,
- in synchronized manner with the programme, transmission takes place of entitlement checking messages individual to each of these programmes, said messages being able to permit descrambling and restoration of the programmes in receivers having the corresponding access or entitlement rights,
- transmission also takes place of partial entitlement checking messages to at least certain of these programmes, said partial entitlement checking messages being able to permit the descrambling and partial restoration of the corresponding programmes for receivers having a partial access or entitlement right.

Advantageously, for performing this process, the information flow corresponding to each programme is broken down into a first, so-called elementary flow, corresponding to a programme which, once restored in a receiver, will be discernible without being directly usable, and a second, so-called complimentary flow making it possible to complete the first flow, in order to permit the complete restoration of the programme. In this variant, the partial entitlement checking messages apply to the elementary flows.

The technical problem which the present invention aims at solving is the production of the elementary flow and the complimentary flow required in said process and this takes place from a single flow leaving a random coder.

DESCRIPTION OF THE INVENTION

Thus, the present invention more particularly relates to the transmission process for programmes with progressive conditional access, namely the stage of forming the elementary and complimentary flows. The invention applies in the case where the information flow leaving the coder is of the digital type, because it is in this case that the most difficult problems occur for progressive conditional access. It is also assumed that the informations are multiplex, i.e. they constitute a "multiplex" formed by a sequence of elements which can be, according to the nature of the multiplexing, frames, packets, etc.

Under these conditions and according to the invention, in order to subdivide the multiplex information flow into an elementary flow and a complimentary flow, alternately groups of m successive elements and p successive elements of the multiplex are taken, the groups of m elements constituting the elementary flow and the groups of p elements the complimentary flow.

Thus, more specifically, the present invention relates to a process for the broadcasting of programmes with progressive conditional access, in which:

- an information flow corresponding to one component of a programme is broken down into a first or elementary flow and into a second or complimentary flow,
- at least the complimentary flow is scrambled with the aid of a control or check word,
- in synchronous manner with each programme, transmission takes place of entitlement checking messages making it possible to descramble and restore the scrambled flows in receivers having the corresponding access or entitlement rights, the restoration of the elementary flow alone leading to a programme component which is discernible without being directly usable and the descrambling of the complimentary flow making it possible to complete the component of the programme in order to permit complete programme restoration,
- said process being characterized in that, the information flow being in the form of a digital multiplex constituted by a sequence of elements, the elementary flow is formed by taking said multiplex groups of m successive elements and the complimentary flow is formed by taking in the multiplex groups of p successive elements, the groups of m successive elements alternating with the groups of p successive elements.

In a first embodiment, the elements of the multiplex are fixed length frames, broken down into variable length channels, the component of the programme to be scrambled being transmitted in a channel of a given order, the elementary flow then being formed by taking the informations contained in a channel of a given order i in groups of m

successive frames and the complimentary flow by the informations contained in the channel of the same given order i in groups of p successive frames alternating with said groups of m successive frames.

In a first variant, scrambling takes place of the channel of given rank i of groups of m successive frames by a first control word CW1 and the channel of the same order i of groups of p successive frames by a second control word CW2.

The control word CW1 can be the known, local control word of the receiver or a control word conveyed within an entitlement checking message.

In another variant, scrambling does not take place of the channel of given order i of the groups of m successive frames and instead scrambling takes place of the channel of given order i of the groups of p successive frames by a control word (CW2).

In a second embodiment, the elements of the multiplex are packets and the elementary flow is formed by the informations contained in the groups of m successive packets and the complimentary flow by informations contained in groups of p successive packets alternating with the groups of m successive packets.

In a first variant, scrambling takes place of the packets of the groups of m successive packets by a first control word CW1 and the packets of the groups of p successive packets by a second control word CW2.

In a second variant, scrambling does not take place of the packets of the groups of m successive packets and instead scrambling takes place of the packets of the groups of p successive packets by a control word (CW2).

The present invention also relates to a receiver able to receive the programmes transmitted according to the process defined hereinbefore. This receiver is characterized in that it incorporates:

- means for subdividing in the information flow received a first or elementary flow constituted by groups of m successive elements and a second or complimentary flow constituted by groups of p successive elements, the groups of m successive elements alternating with the groups of p successive elements,
- means for recognizing at least one entitlement checking message in the informations received and for extracting therefrom at least one control word and at least one access condition,
- means for checking if at least said access condition is satisfied,
- means for descrambling at least the complimentary flow with the aid of the associated control word if the corresponding access condition is satisfied,
- at least one video, audio or data receiver receiving at least the signals of the elementary flow and, if appropriate, the signals of the descrambled complimentary flow if the corresponding access condition is satisfied.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram showing a pay television broadcasting network

FIG. 2 is a diagram showing the organization of a multiplex according to the frame multiplexing method.

FIG. 3 is a diagram showing the organization of a multiplex according to the packet multiplexing method.

FIG. 4 illustrates the constitution of the elementary flow and the complimentary flow in the case of a frame multiplex

FIG. 5 shows the respectively scrambled, degraded and descrambled components in the preceding case

FIG. 6 illustrates the means making it possible to perform the process of the invention in the case of frame multiplexing.

FIG. 7 illustrates the constitution of the elementary flow and the complimentary flow in the case of a packet multiplex.

FIG. 8 shows the respectively scrambled, degrade and descrambled components in the preceding case.

FIG. 9 illustrates the means making it possible to perform the process of the invention in the case of packet multiplexing.

FIG. 10 shows the block diagram of a receiver able to process signals broadcast according to the process of the invention.

FIG. 11 illustrates the operation of the demultiplexer-descrambler in the case of a frame multiplex.

FIG. 12 illustrates the operation of the demultiplexer-descrambler in the case of a packet multiplex.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

FIG. 1 shows a conventional pay television programme broadcasting network or link having, on the transmission side, source coders in the form of two coders **10**, **10'**, a multiplexer/scrambler **12** and, on the reception side, a demultiplexer/descrambler **14** and source decoders in the form of the two decoders **18**, **18'**.

The information flows from the source coders **10**, **10'** supply the multiplexer/scrambler **12**, which multiplexes and scrambles said flows in order to supply a single flow constituting the broadcast flow.

Scrambling is a reversible operation for transforming the signal transmitted with the aid of a key called a check or control word (CW), in order to make said programme unintelligible for users not having said control word.

In order to permit descrambling, the control word is transmitted in encrypted form in entitlement checking messages (ECM). Each ECM also contains the access condition (EC) to be satisfied by the access control module of the user in order to permit the decrypting of the control word CW and consequently the descrambling of the signal.

The control words have a limited life of typically 10 seconds. In order to avoid any problem during control word changes, the respectively current and future control words are transmitted in the entitlement checking message, one being the even control word used during an even phase and designated CW_e, whilst the other is the odd control word CW used during an odd phase.

The information flows from the source coders are time multiplexed. Two methods are mainly used in the field of digital broadcasting, namely frame multiplexing and packet multiplexing.

In frame multiplexing, the multiplex is constituted by a succession of frames of fixed length all having the same organization, as indicated in the diagram of FIG. 2, which shows a frame of order i and the following frame of order i+1.

A frame is broken down into n variable length channels. Each channel conveys an elementary flow (video, sound, etc.). The same breakdown is used for all the frames (multiplex reconfigurations are possible, but rare). The flow rate allocated to a channel of order k is equal to (Lgk)/Tbits/s, in which Lgk is the length of the channel k in bits and T the period of the frame.

In exemplified manner, reference can be made to the STERNE multiplex, which is a frame multiplex The length of a frame is 24 ms. The flow rate allocated to a channel which would have a length of 1 byte would be equal to approximately 333 bits/s.

In general, one channel is reserved for conveying a service link describing all the other channels of the frame: channel length, description of the elementary flow conveyed in the channel, scrambling and access control parameters, etc.

The service link also conveys a frame counter e.g. used for fixing the life of the control words and the parity of the phase.

At present, the scrambling of an elementary flow takes place by scrambling, in all the frames, all the bits of the channel conveying the elementary flow. In FIG. 2, the scrambling relates to channel 2 and is symbolized by hatching.

Packet multiplexing consists of producing a succession of fixed or variable length packets. Each packet contains the data of an elementary flow. The diagram of FIG. 3 gives an example of packet multiplex, conveying three elementary flows A, B and C. Each packet is constituted by a header (E-T), a data field and a suffix (Sfx).

At present, the scrambling of an elementary flow takes place by scrambling all the data fields of packets conveying said elementary flow. In the example illustrated in FIG. 3, only the elementary flow B is scrambled (the hatching symbolizing scrambling).

In exemplified manner, the multiplex MPEG2 is a packet multiplex in which the packets all have a fixed length of 188 bytes. The header contains an identifier of the elementary flow, plus two bits defining the scrambling parameters and method used for this packet. The values of these two bits are at present standardized:

00: no scrambling

01: reserve

10: scrambling with the even control word

11: scrambling with the odd control word.

In the aforementioned patent application 92 15841 (U.S. Ser. No. 08/172,817), a description is given as to how a progressive scrambling mechanism can be implemented in the case where the video or audio component is in two discernible flows. In this case, it is sufficient to apply a control word CW1 (associated with an access condition CA1) to the elementary flow and a control word CW2 (associated with an access condition CA2) to the complimentary flow. The access condition CA1 and the cryptogramme (cipher text) of CW1 are conveyed in an entitlement checking message ECM1. The access condition CA2 and the cryptogramme of CW2 are conveyed in an entitlement checking message ECM2. The access condition CA1 alone permits the descrambling of the elementary flow, thus supplying a picture or sound in degraded, but comprehensible form for the user.

A description will now be given as to how it is possible to produce two discernible flows, respectively scrambled with the control word CW1 and CW2, in the case of a frame multiplex and a packet multiplex.

In the case of the frame multiplex, the component to which it is wished to apply the progressive scrambling is transmitted in channel i of each frame. The process of the invention then consists of scrambling the channel i of m successive frames with the word CW1 and then the same channel of p successive frames with CW2, followed by the same channel of m successive frames with CW1, etc., as indicated in FIG. 4, where the vertical lines symbolize a scrambling with CW1 and the horizontal lines a scrambling with CW2. The words CW1 and CW2 change parity at the same time. This parity is not indicated in the diagram of FIG. 4.

The values of the quantities m and p, individual to each of the scrambled channels must be known by the decoder in implicit or explicit manner. In the latter case, they are transmitted in the service link, accompanied by a synchronization information (e.g. a particular value of the frame counter) indicating at which frame the scrambling commences with CW1 or CW2.

On reception, the elementary flow is obtained by descrambling the frames scrambled with CW1. The complimentary flow is obtained by descrambling the frames scrambled with CW2. The delivery to the video or audio decoder of a single elementary flow gives a picture or a sound in degraded form. The delivery to the video or audio decoder of the elementary flow accompanied by the complimentary flow gives a top quality picture or sound.

FIG. 5 shows on the first line the scrambled component and on the second line the degraded component when only the elementary flow has been descrambled and on the third line the completely descrambled component.

The choice of the quantities m and p must be fixed as a function of the performance characteristics of the video or audio decoder and in particular as a function of its lock-in time. In general, m is well above p, because very few scrambled frames are required in order to greatly disturb the behaviour of the video or audio decoder.

The means used on transmission are shown in FIG. 6. They comprise a multiplexer 20 with a first output 21 supplying uncoded data, a second output supplying the frame synchronization, a third output supplying the quantities m and p, as well as the frame counter and the parity, and finally a fourth output 24 supplying two entitlement checking messages ECM1, ECM2.

The means also comprise a circuit 25 containing the control words used (CW1 even and odd and CW2 even and odd) and the scrambler 26, which uses one or other of these words. The circuit 25 supplies on a first output 27 the scrambled data, on a second output 28 the frame synchronization and on a third output 29 the quantities m and p, as well as the frame counter and parity.

As it is now a question of packet multiplex, the case is close to that of the frame multiplex, the difference being based on the transmission of the synchronization informations between the scrambler and the descrambler. Thus, in the case of the packet multiplex, the packet header can be used for conveying the information. It is in the packet header which will be supplied the scrambling information with CW1 or CW2, as well as the parity, This more particularly makes it possible for the scrambler to vary the values of m and p.

For example, the quantity m can correspond to the number of packets necessary for encoding an intra picture, whereas p can correspond to the number of packets between two intra pictures.

It is pointed out that the scrambling of the elementary flow with the control word CW1 is not obligatory. In a simplified variant, the channel of order i of groups of m successive frames is not scrambled and scrambling only takes place of the channel of order i of groups of p successive frames and this takes place with the control word CW2. Thus, no definition takes place of the access conditions CA1 and the control word CW1 is not used. This amounts to exerting no

control on the reception of the elementary flow and to offering all receivers access to the picture or sound in degraded form.

It is also pointed out that, as hereinbefore, the control word CW1 can be a known, local control word of the receiver or a control word conveyed within an entitlement checking message.

FIG. 7 shows how the elementary flow is formed with groups of m packets, which will be scrambled with the first control word CW1 and groups of p packets, which will be scrambled with the second control word CW2. The vertical lines symbolize the scrambling with CW1 and the horizontal lines the scrambling with CW2.

On reception, the elementary flow will be obtained by descrambling the packets scrambled with CW1. The complimentary flow will be obtained by descrambling the packets scrambled with CW2. The delivery to the video or audio decoder of an elementary flow only will give a degraded sound or picture. The delivery to the video or audio decoder of the elementary flow accompanied by the complimentary flow will give a top quality picture or sound.

FIG. 8 shows on the first line the scrambled component, on the second line the degraded component corresponding to the descrambled elementary flow only, and on the third line the completely descrambled component (elementary and complimentary flows).

Here again, the choice of m and p must be fixed as a function of the performance characteristics of the video or audio decoder and in particular as a function of its lock-in time. Generally, m greatly exceeds p, because very few scrambled packets are required for greatly disturbing the behaviour of the video or audio decoder.

FIG. 9 diagrammatically shows the means used on transmission, in the packet multiplexing variant. These means comprise a multiplexer 30 supplying on a first output 31 the uncoded packets, on a second output 32 the packet synchronization, on a third output 33 the quantities m and p, as well as the parity and on a fourth output 34 the entitlement checking messages ECM1, ECM2.

These means also comprise a circuit 35 containing the even and odd control words CW1 and the even and odd control words CW2 and the scrambler 36 using said words. The circuit 35 supplies on a first output 37 the scrambled packets and on a second output 38 a parity signal.

In both packet and frame multiplexing, a particular implementation of the present process consists of not defining an access condition CA1 and not using the control word CW1. This amounts to exerting no control on the reception of the elementary flow and offering all receivers access to the degraded picture or sound. It is also possible to use as the control word CW1, the known, local control word of the receiver or a control word conveyed within an entitlement checking message.

Finally, it is possible to define a manner of implementing the process of the invention in the case of so-called MPEG2 multiplexing. In the particular case of MPEG2, the indication for the scrambling in the header of each packet is constituted by two bits called "Transport-Scrambling-Control" (TSC) in the draft standard MPEG2 system (ISO/IEC CD 13818-1). The values of these two bits are at present standardized:

00: the packet is not scrambled

01: is reserved

10: the packet is scrambled with the even control word

11: the packet is scrambled with the odd control word.

In order to implement the process described hereinbefore, it is necessary to be able to indicate to the decoder no longer two control words (even or odd) but in all four control words (CW1 even, CW2 even, CW1 odd, CW2 odd). It must be able to indicate which of these four control words has been used for scrambling the data field of the packet and for this purpose it is possible to use the value "01", which is at present reserved.

The behaviour of the decoder is then as follows (the behaviour of the coder being easily deduced therefrom). It is assumed that the decoder has a parity memory (1 bit sufficient) called MEM-PAR:

- initial state: MEM-PAR=0 or 1
- reception of a packet with TSC="00": no descrambling action to take place
- reception of a packet with TSC="10": descrambling of the packet with CW2 even and MEM-PAR→0 (i.e. storing the value "0" in MEM-PAR)
- reception of a packet with TSC="11": descrambling of the packet with CW2 odd and MEM-PAR→1 (i.e. storing the value "1" in MEM-PAR)
- reception of a packet with TSC="01": descrambling of the packet with CW1 even if MEM-PAR=0 or with CW1 odd if MEM-PAR=1.

On connecting the receiver, the content of the parity memory MEM-PAR has a ½ probability of being erroneous up to the reception of the first packet with TSC="10" or "11". The maximum waiting time before being perfectly synchronized is m packets. It is therefore necessary in the implementation of this variant to ensure that this time delay is not perceptible for the user (lowest possible value of m).

It is pointed out that the particular case of implementing the process consisting of not defining the access condition CA1 and not using the control word CW1 can easily be brought about by using the value TSC="00" instead of TSC="01".

The decoder solely having access to the degraded picture can operate according to several modes:

- supply to the video decoder the descrambled pictures, as well as the pictures remaining scrambled,
- deliver to the video decoder only the descrambled pictures and the video decoder freezes the last picture received during the reception of the scrambled pictures.

FIG. 10 diagrammatically illustrates a receiver able to receive the programmes transmitted in accordance with the process which has been described. In FIG. 10 the receiver carries the general reference 40. This receiver has a general input 41, a demodulator 42, a demultiplexer/descrambler 44, a security processor 46, video decoder 48, an audio decoder 50, a data decoder 52, a display screen 54, a loudspeaker 56 and a personal computer 58.

The signal received on the input 41 is firstly demodulated in the circuit 42 and is then supplied to the demultiplexer/descrambler 44, which extracts the frames or packets of the selected component and descrambles them if the user has the requisite access rights,

The signal is then supplied to the video decoder 48 in the case of a video signal, to the audio decoder 50 in the case of an audio signal, or to a data decoder 52 in the case of a data signal. Once the signal has been decoded, it is supplied to the user on the appropriate support, namely screen 54 for video, loudspeaker 56 for audio and computer 58 for data.

In the case of a frame multiplex, the demultiplexer/descrambler 44 is organized in accordance with FIG. 11. The general input E is connected to a frame demultiplexer 60 having three outputs respectively 61 for the scrambled data, 62 for the frame synchronization and 63 for the quantities m and p, the frame counter and parity.

The descrambler 64 either receives even control words CW1, CW2, or odd control words CW1, CW2 according to the parity and descrambles the signals. The uncoded signals are available on the output S.

The demultiplexer/descrambler analyzes the service link in order to restore there (if it does not know them in implicit manner) the values of m, p and the synchronization information indicating at what frame the scrambling commences with CW1 or CW2.

The demultiplexer/descrambler restores ECM1 and ECM2. It supplies said ECM to the security processor of the decoder (often a microprocessor card) for checking the access conditions CA1 and CA2 and calculating the control word CW1 and CW2 if the access conditions are respected. If the user satisfies neither CA1 nor CA2, the component remains entirely scrambled.

If the user satisfies the access condition CA1, but not the access condition CA2, he has access to a picture or a sound or data in degraded form. The demultiplexer/descrambler descrambles bursts of m frames scrambled with CW1. He thus produces a flow constituted by m uncoded frames, then p coded frames, then again m uncoded frames, etc. This flow is supplied to the video or audio or data decoder.

If the component is an audio component, the audio decoder can decode everything (the decoding of the scrambled frames leading to noise on the loudspeaker) or can decide not to decode the bursts of p frames remaining scrambled (no sound on the loudspeaker during the passage of these frames).

If the component is a video component, the video decoder can decode everything (the decoding of the scrambled frames leading to a noisy picture on the screen) or can decide not to decode the bursts of p frames remaining scrambled and freeze on the screen during this time the last correctly decoded picture.

If the user satisfies the access conditions CA1 and CA2, he has access to a picture or a sound or data in completely descrambled form.

The demultiplexer/descrambler descrambles the bursts of frames scrambled with CW1 and the bursts of p frames scrambles with CW2. He thus produces a flow constituted by completely descrambled frames and this flow is supplied to the video or audio or data decoder.

A particular case consists of not defining the access condition CA1 and not using the control word CW1 (the bursts of m frames are uncoded). This amounts to exerting no control on the reception of the elementary flow and offering all receivers access to the degraded sound or picture.

In the case of a packet multiplex, the demultiplexer/descrambler 44 is organized according to FIG. 12. The input E' is connected to a packet demultiplexer 60' having three outputs, respectively 61' supplying the scrambled packets, 62' for packet synchronization and 63' for the quantities m and p and for parity.

The descrambler 64' receives either the even control word CW1 or CW2, or the odd control word CW1, CW2, according to the parity, and descrambles the signals. The uncoded signals are available on the output S'.

The demultiplexer/descrambler restores ECM1 and ECM2 and supplies them to the security processor of the decoder (often a microprocessor card) for checking the access conditions CA1 and CA2 and calculating the control word CW1, CW2 if the access conditions are respected. If the user satisfies neither CA1 nor CA2, the component remains entirely scrambled.

The demultiplexer/descrambler analyzes the header of the packets in order to know with which CW he must descramble the packet (CW1 even, CW1 odd, CW2 even, CW2 odd).

If the user satisfies access condition CA1, but not access condition CA2, he has access to a picture, or sound or data in degraded form in accordance with the mechanism indicated below.

The demultiplexer/descrambler descrambles the bursts of n packets scrambled with CW1. It thus produces a flow constituted by m uncoded packets, then p scrambled packets, then again m uncoded packets, etc. This flow is supplied to the video or audio or data decoder.

If the component is an audio component, the audio decoder can decode everything (the decoding of the scrambled packets leading to noise on the loudspeaker) or may decide not to decode the bursts of p packets remaining scrambled (no sound on the loudspeaker during the passage of these packets).

If the component is a video component, the video decoder can decode everything (the decoding of the scrambled packets leading to a noisy picture on the screen) or may decide not to decode the bursts of p packets remaining scrambled and freeze on the screen during this time the final correctly decoded picture.

If the user satisfies the access conditions CA1 and CA2, he has access to a picture, sound or data in completely descrambled form.

The demultiplexer/descrambler descrambles the bursts of packets scrambled with CW1 and the bursts of packets scrambled with CW2. He thus produces a flow constituted by completely descrambled packets. This flow is supplied to the video, audio or data decoder.

A particular implementation case consists of not defining the access condition CA1 and not using the control word CW1 (the bursts of m packets being uncoded). This amounts to exerting no control on the reception of the elementary flow and offering all receivers access to the degraded picture or sound.

We claim:

1. A method for broadcasting programs with progressive conditional access, comprising the steps of:

breaking an information flow of a program into a first flow and a second flow, said breaking step comprising,

arranging said first flow into a channel of order i in groups of m successive fixed length frames, said fixed length frames comprising variable length channels arranged in plural orders,

arranging said second flow into the channel of order i in groups of p successive fixed length frames;

scrambling the second flow with a control word; and

transmitting an entitlement checking message with said program so that a receiver equipped with an access right may descramble and restore the information flow, reception of the first flow resulting in a partially discernable program and reception of said second flow, once descrambled, resulting in complete restoration of the program, said transmitting step comprising the steps of,

transmitting said program in said channel of order i, and

multiplexing said groups of m successive fixed length frames alternately with said groups of p successive fixed length frames.

2. The process according to claim 1, wherein said scrambling step comprises the steps of:

scrambling the groups of m successive fixed length frames of said first flow by another control word; and

scrambling the groups of p successive fixed length frames of the second flow by the control word.

3. The process according to claim 2, wherein said step of scrambling the groups of m successive fixed length frames comprises scrambling the groups of m successive fixed length frames with the another control word which comprises at least one of a known control word of the receiver and a transmitted control word that is conveyed within the entitlement checking message.

4. The process according to claim 1, wherein said step of transmitting an entitlement checking message comprises:

transmitting said said program in a channel of order i of said variable length channels, where said groups of m successive fixed length frames of said first flow comprise m unscrambled frames and said p successive elements of said second flow comprise p scrambled frames.

5. The process according to claim 2 or 4, wherein said step of transmitting an entitlement checking message comprises the steps of:

transmitting numbers corresponding to respective values of m and of p; and

transmitting indicia regarding which of said groups of m successive fixed length frames and said group of p successive fixed length frames is a first scrambled frame and which of said control word and said another control word scrambled the first scrambled frame.

6. A method for broadcasting programs with progressive conditional access, comprising the steps of:

breaking an information flow of a program into a first flow and a second flow, said breaking step comprising,

arranging said first flow into a channel of order i in groups of m successive packets, and

arranging said second flow into the channel of order i in groups of p successive packets;

scrambling the second flow with a control word; and

transmitting an entitlement checking message with said program so that a receiver equipped with an access right may descramble and restore the information flow, reception of the first flow resulting in a partially discernable program and reception said second flow, once descrambled, resulting in complete restoration of the program, said transmitting step comprising,

multiplexing said groups of m successive packets alternately with said groups of p successive packets.

7. The method according to claim 6, wherein said scrambling step comprises scrambling said groups of m successive packets by another control word.

8. The method according to claim 7, wherein said step of scrambling said groups of m successive packets comprises scrambling with the another control, where said another control word comprises at least one of a known control word of the receiver and a transmitted control word conveyed within the entitlement checking message.

9. The method according to claim 6, wherein said step of transmitting comprises:

transmitting said group of m successive packets as unscrambled packets and said group of p successive packets as scrambled packets.

10. The method according to claim 7 or claim 9, wherein:

said breaking step comprises,

arranging said first flow into a channel of order i in groups of said m successive packets, each packet comprising a header, and

arranging said second flow into the channel of order i in groups of said p successive packets, each packet comprising the header; and

said transmitting step comprising,

transmitting indicia regarding which of said control word and said another control word is transmitted in the header of respective of said m successive packets and said p successive packets.

11. The method according to claim 6, wherein:

said step of arranging said first flow into the channel of order i in groups of m successive packets comprises arranging said first flow where m is a variable; and

said step of arranging said second flow into the channel of order i in groups of p successive packets comprises arranging said second flow where p is a variable.

12. The method of claim 2, wherein:

said scrambling step comprises scrambling with said another control word and said control word, said another control word and said control word having respective limited phases;

said multiplexing step comprises alternately multiplexing said groups of m successive fixed length frames and said p successive fixed length frames with an even phase and an odd phase;

said step of transmitting an entitlement checking message comprises transmitting at least one of said control word and said another control word as a current control word of a current phase and a future control word of a following phase, one of said current word and said future control word being called an even word used during an even phase and the other of being called an odd word used during an odd phase, comprising,

changing respective parities of the another control word and the control word at a same time,

using the even word and the odd word relative to the control word,

using the even and odd words relative to the another control word, and

transmitting a parity information about the even and odd words used.

13. The method of claim 7, wherein:

said scrambling step comprises scrambling with said another control word and said control word, said another control word and said control word having respective limited phases;

said multiplexing step comprises alternately multiplexing said groups of m successive packets and said p successive packets with an even phase and an odd phase;

said step of transmitting an entitlement checking message comprises transmitting at least one of said control word and said another control word as a current control word of a current phase and a future control word of a following phase, one of said current word and said future control word being called an even word used during an even phase and the other of being called an odd word used during an odd phase, comprising,

changing respective parities of the another control word and the control word at a same time,

using the even and odd words relative to the control word,

using the even and odd words relative to the another control word, and

transmitting a parity information about the even and odd words used.

14. A receiver for receiving programs transmitted with progressive conditional access, comprising:

means for subdividing a transmitted information flow into a first flow of m successive elements and a second flow of p successive elements, the respective groups of m successive elements alternating with the groups of p successive elements;

means for recognizing at least one entitlement checking message in the transmitted information flow and for extracting therefrom at least one control word and at least one access condition;

means for checking if said at least said one access condition is satisfied by said receiver;

means for descrambling at least the second information flow using said at least one control word if the at least one of said access condition is satisfied as checked by said means for checking; and

at least one of a video, an audio and a data receiver configured to receive at least the second flow of p successive elements and a descrambled complimentary flow corresponding to said second flow of p successive elements if the access condition is satisfied.

15. The receiver according to claim **14**, wherein:

said means for recognizing the at least one entitlement checking message comprises means for recognizing two entitlement checking messages and restoring two control words and two access conditions;

said means for checking if said at least one access condition is satisfied comprises means for checking if the two access conditions are satisfied; and

said means for descrambling at least the second information flow comprises means for descrambling the first information flow based on the first control word.

16. The receiver according to claim **14**, wherein:

said means for recognizing at least one entitlement checking message comprising means for recognizing a single entitlement checking message and restoring a single control word and a single access condition;

said means for checking if at least one access condition is satisfied checks only whether one of said at least one access condition is satisfied; and

said means for descrambling at least the second information flow solely descrambles the second information flow using a single restored control word of the at least one control word.

17. The receiver according to claim **16**, wherein the means for descrambling at least the second information flow comprises means for descrambling the first information flow based on a known control word of the receiver.

18. The receiver according to claim **14**, wherein:

said means for recognizing at least one entitlement checking message comprises means for extracting four control words comprising first and second even words and first and second odd words; and

the receiver further comprises,

a parity memory with at least one bit, and

means for recognizing a state of a group of two received bits.

19. The receiver as in one of the claims **14–18** wherein said at least one of a video, an audio, and a data receiver receives both descrambled signals and scrambled signals.

20. The receiver as in one of the claims **14–18**, wherein said at least one of a video, an audio, and data receiver only receives descrambled signals.

* * * * *

US005594794A

United States Patent [19]

Eyer et al.

[11] Patent Number: 5,594,794

[45] Date f Patent: Jan. 14, 1997

[54] METHOD AND APPARATUS FOR FREE PREVIEWS OF COMMUNICATION NETWORK SERVICES

[75] Inventors: Mark Eyer, San Diego; Allen Shumate, Poway; Paul Moroney, Olivenhain, all of Calif.

[73] Assignee: General Instrument Corporation of Delaware, Chicago, Ill.

[21] Appl. No.: 324,591

[22] Filed: Oct. 18, 1994

[51] Int. Cl.[6] H04L 9/00

[52] U.S. Cl. 380/20; 380/21

[58] Field of Search 380/20, 21

[56] References Cited

U.S. PATENT DOCUMENTS

4,613,901	9/1986	Gilhousen et al.	380/20
4,739,510	4/1988	Jeffers et al.	380/20
4,864,615	9/1989	Bennett et al.	380/20
5,091,938	2/1992	Thompson et al.	380/21
5,311,325	5/1994	Edwards et al.	380/20
5,323,462	6/1994	Farmer	380/20

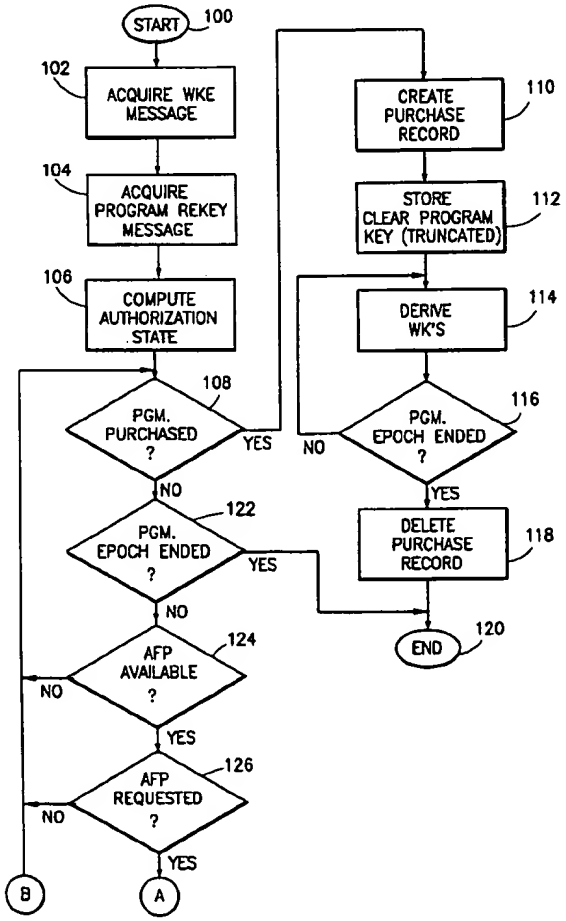
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—Barry R. Lipsitz; Ralph F. Hoppin

[57] ABSTRACT

Limited duration previews of program offerings available for purchase via a communication network are provided in a cryptographically secure manner at virtually any time during the service. The invention has particular applicability to the provision of video services on a pay-per-view basis. Such a video service is provided during a program epoch. A fixed period is defined during the program epoch when portions of the video service are available for viewing on a preview basis. A consumer is allowed to preview, without purchase, portions of the video service at any time during the fixed period for up to a maximum preview duration that is shorter than the fixed period. The consumer can then purchase the video service for viewing during the program epoch after previewing portions thereof. A plurality of records is maintained to service different previewable programs concurrently.

29 Claims, 5 Drawing Sheets



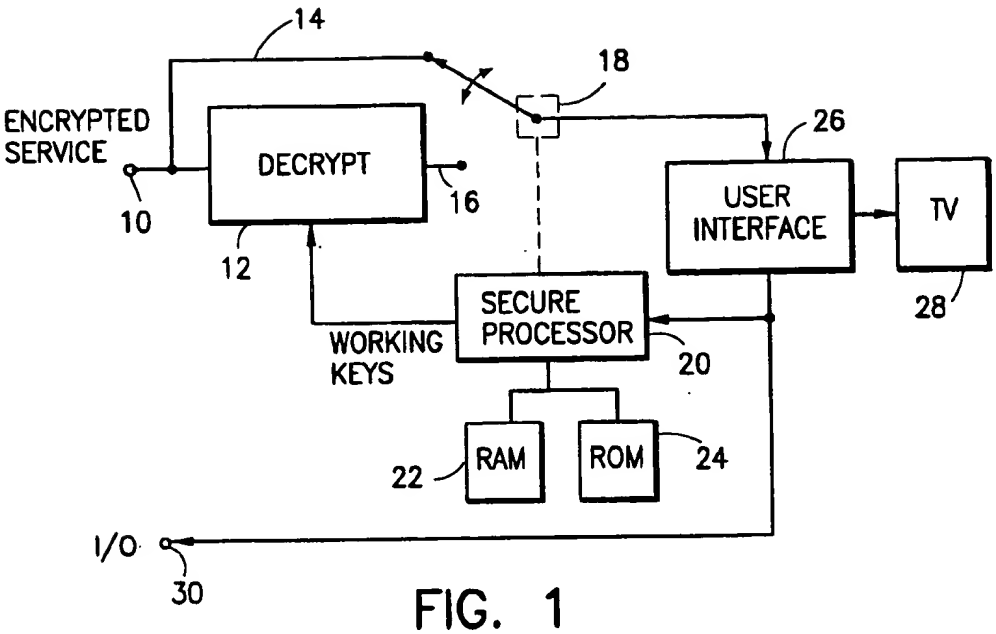

14
18
ENCRYPTED SERVICE
DECRYPT
26
USER INTERFACE
TV
10
16
12
28
SECURE PROCESSOR
WORKING KEYS
20
RAM
ROM
22
24
I/O
30

FIG. 1

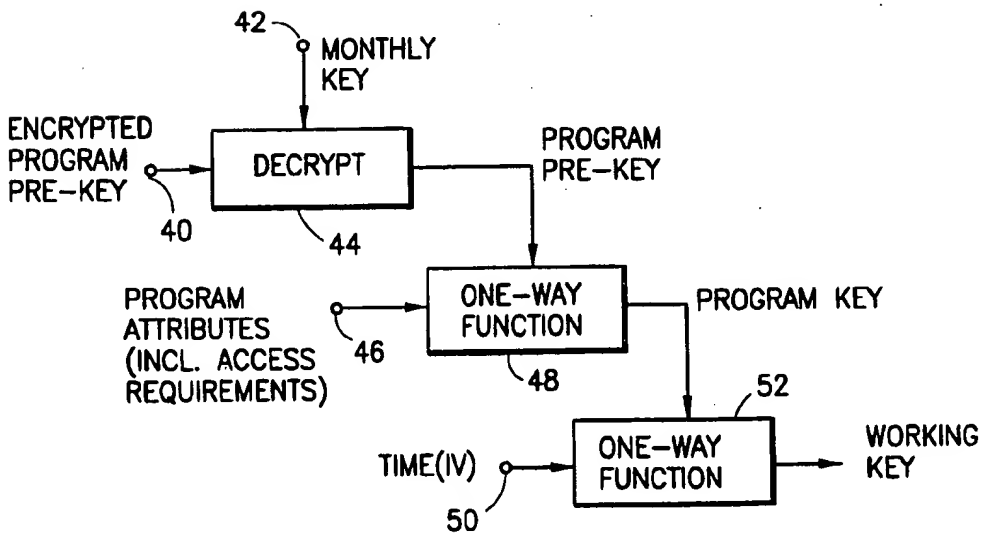

42
MONTHLY KEY
ENCRYPTED PROGRAM PRE-KEY
DECRYPT
PROGRAM PRE-KEY
40
44
PROGRAM ATTRIBUTES (INCL. ACCESS REQUIREMENTS)
ONE-WAY FUNCTION
PROGRAM KEY
46
48
52
TIME(IV)
ONE-WAY FUNCTION
WORKING KEY
50

FIG. 2

FIG. 3

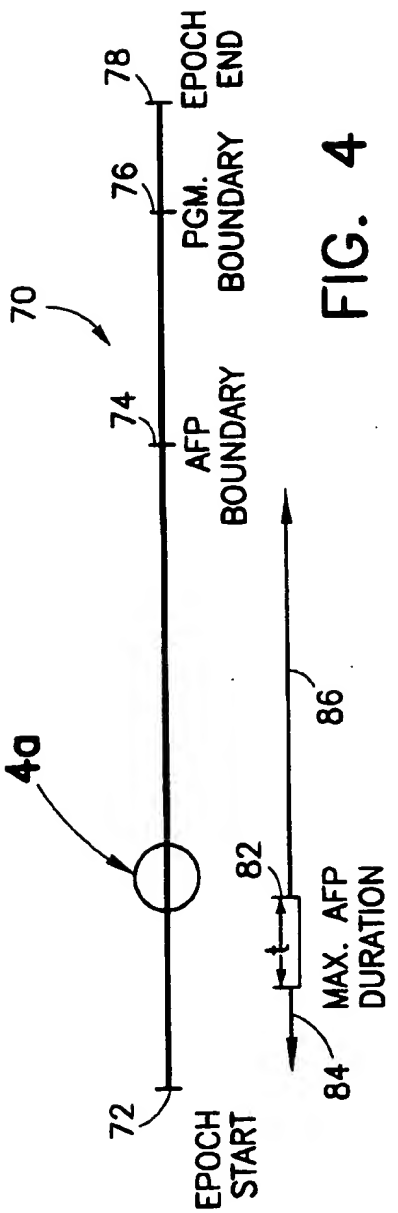


FIG. 4

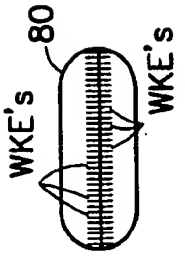


FIG. 4a

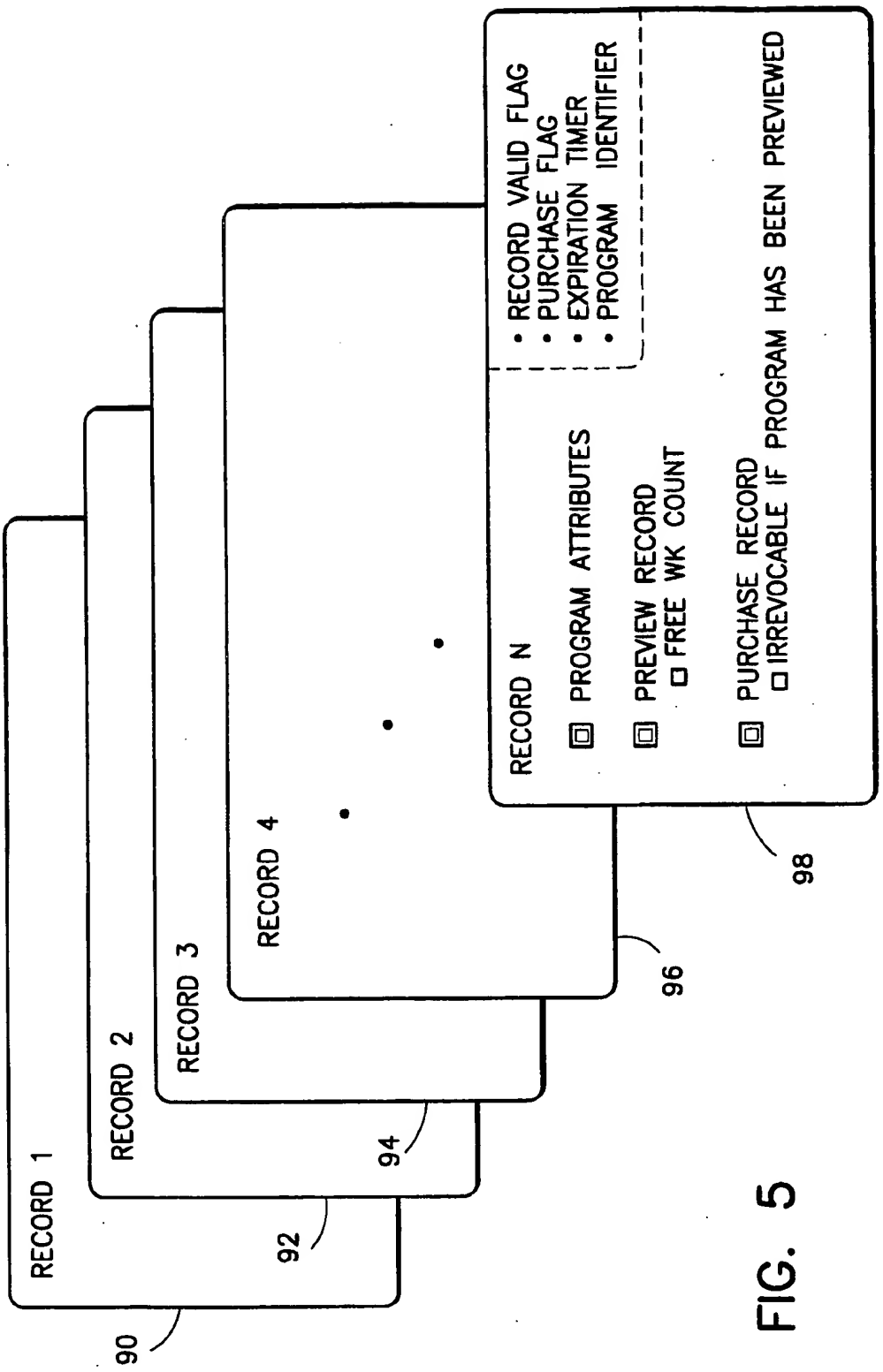

RECORD 1
RECORD 2
RECORD 3
RECORD 4
RECORD N
• RECORD VALID FLAG
• PURCHASE FLAG
• EXPIRATION TIMER
• PROGRAM IDENTIFIER
PROGRAM ATTRIBUTES
PREVIEW RECORD
FREE WK COUNT
PURCHASE RECORD
IRREVOCABLE IF PROGRAM HAS BEEN PREVIEWED
90
92
94
96
98

FIG. 5

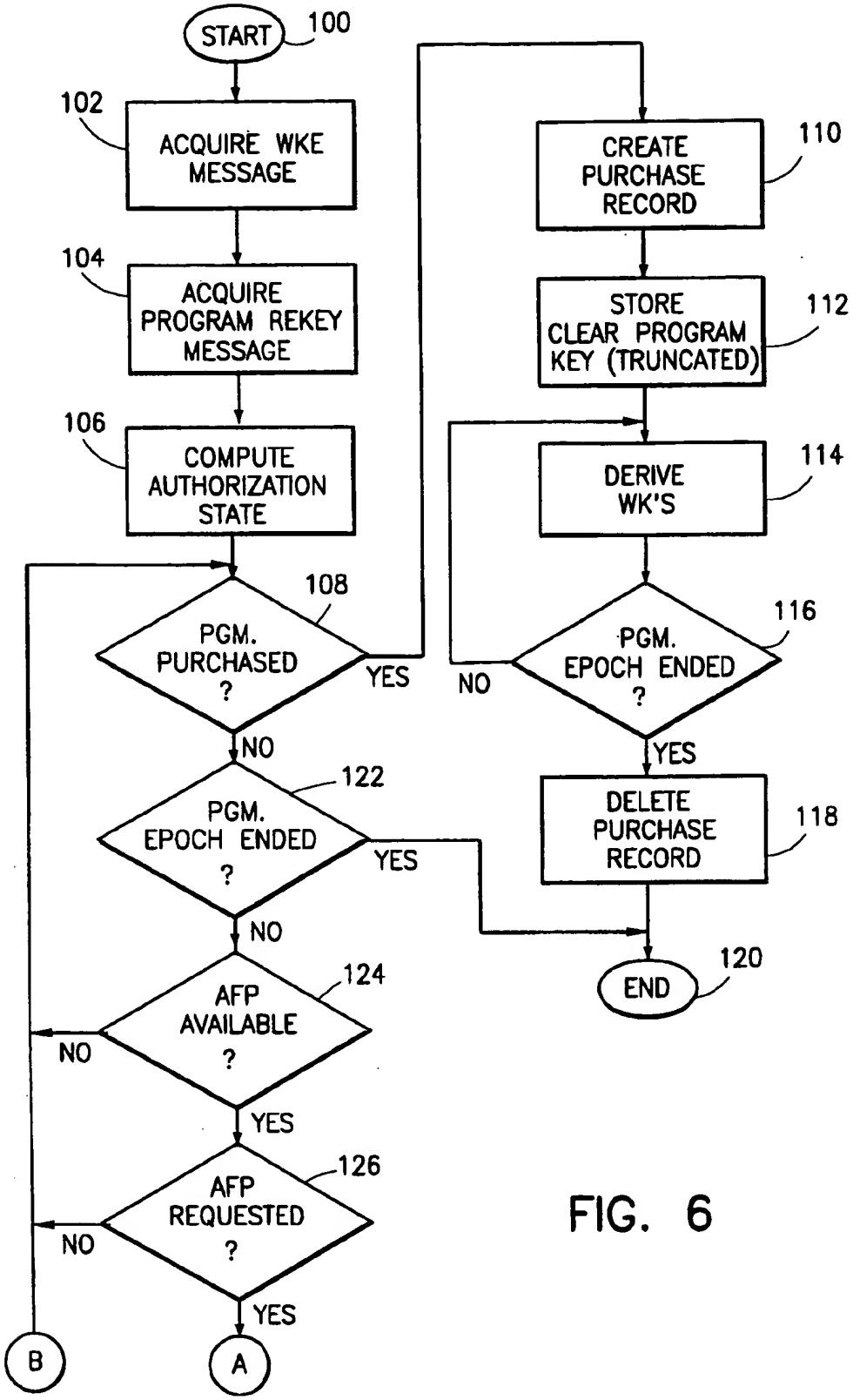
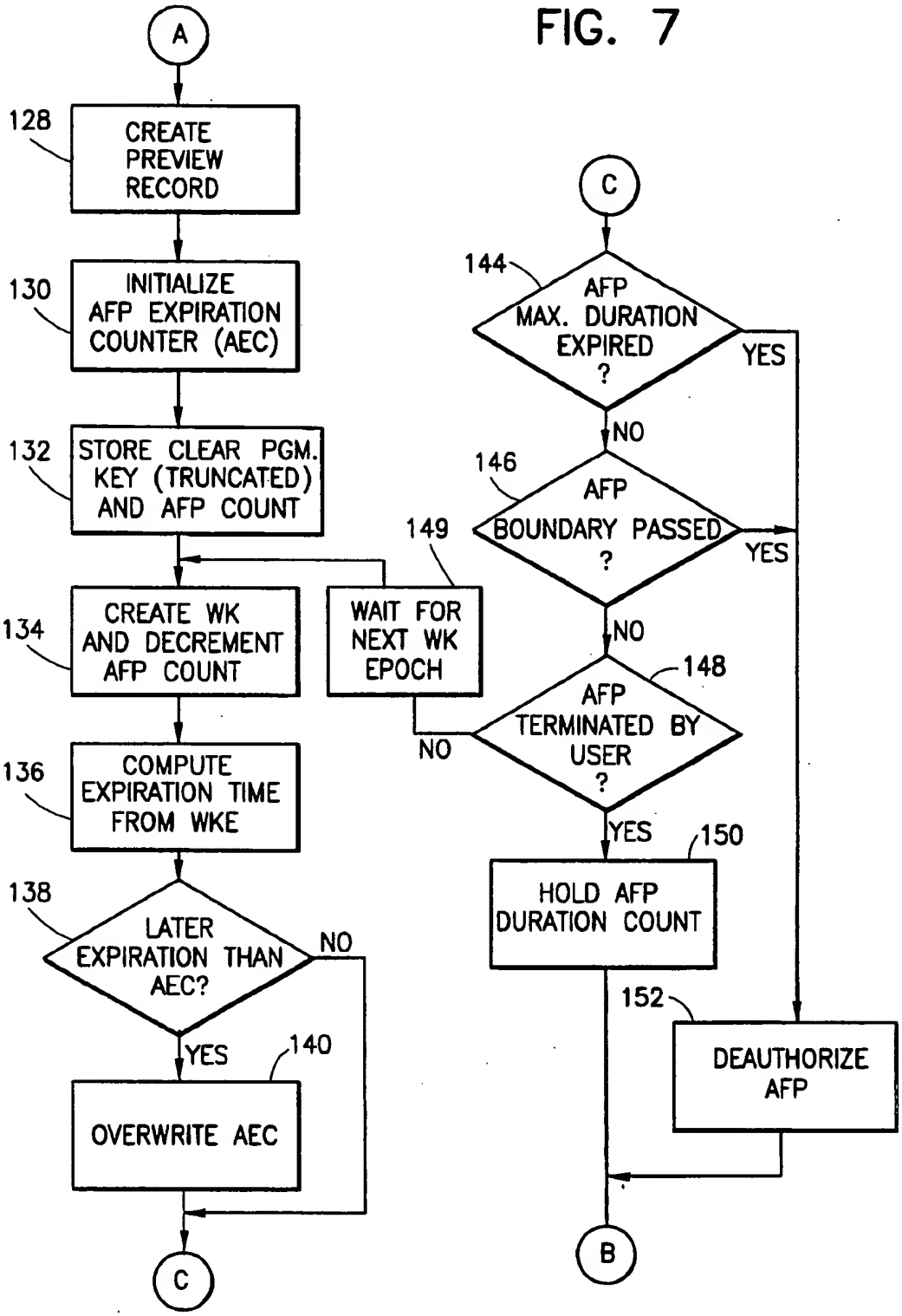

START
100
102
ACQUIRE WKE MESSAGE
104
ACQUIRE PROGRAM REKEY MESSAGE
106
COMPUTE AUTHORIZATION STATE
108
PGM. PURCHASED ?
YES
NO
122
PGM. EPOCH ENDED ?
YES
NO
124
AFP AVAILABLE ?
NO
YES
126
AFP REQUESTED ?
NO
YES
B
A
110
CREATE PURCHASE RECORD
112
STORE CLEAR PROGRAM KEY (TRUNCATED)
114
DERIVE WK'S
116
PGM. EPOCH ENDED ?
NO
YES
118
DELETE PURCHASE RECORD
120
END

FIG. 6

FIG. 7


A
128
CREATE PREVIEW RECORD
130
INITIALIZE AFP EXPIRATION COUNTER (AEC)
132
STORE CLEAR PGM. KEY (TRUNCATED) AND AFP COUNT
134
CREATE WK AND DECREMENT AFP COUNT
136
COMPUTE EXPIRATION TIME FROM WKE
138
LATER EXPIRATION THAN AEC?
NO
YES
140
OVERWRITE AEC
C
149
WAIT FOR NEXT WK EPOCH
C
144
AFP MAX. DURATION EXPIRED ?
YES
NO
146
AFP BOUNDARY PASSED ?
YES
NO
148
AFP TERMINATED BY USER ?
NO
YES
150
HOLD AFP DURATION COUNT
152
DEAUTHORIZE AFP
B

METHOD AND APPARATUS FOR FREE PREVIEWS OF COMMUNICATION NETWORK SERVICES

BACKGROUND OF THE INVENTION

The present invention relates to communications networks such as cable television, satellite television and computer networks over which services are available for a fee, and more particularly to a method and apparatus for providing free previews of individual program offerings (e.g., a movie) prior to purchasing that offering.

Cable and satellite television networks where video services are available for a fee are well known. Also well known are computer network services such as CompuServe, Prodigy, America Online, Dialog Information Service, and others where databases, banking and shopping services can be accessed and e-mail and the like can be communicated, all for a fee. In the past, some communication networks have provided services on a free trial basis. For example, pay per view television movies, in which a viewer can order a movie for viewing upon payment of a fee, have sometimes enabled viewers to watch the first five minutes or so of the movie on a preview basis before purchase is required. Such previews were limited to a predefined time period at the beginning of the movie. Free previews were not available at any other time during the broadcast of the movie.

The provision of a limited free preview at any time during the broadcast of a service (such as a movie) would be desirable from a consumer's standpoint. For video services, a viewer would not be constrained to having a preview only at the beginning of the program, which may not be a convenient time for the viewer. However, the provision of a limited duration free preview at any time during the availability of a service is fraught with danger from the standpoint of the service provider. In particular, opening up a service to free previews at any time may make it possible for an unscrupulous viewer or "pirate" to defeat the security of the signal and obtain the entire service without charge.

It would be advantageous to provide a method and apparatus for allowing a limited duration free preview at virtually any time during the provision of a service. It would be further advantageous to provide such a method and apparatus that are not easily taken advantage of by unscrupulous customers or pirates. Such a method and apparatus should maintain signal security while providing the flexibility of an "anytime free preview" (AFP). It would also be advantageous to provide such a method and apparatus that enable a viewer to switch back and forth between one or more AFPs (each associated with a different service) and conventional programming. Each AFP would be limited to its own particular maximum AFP duration. Such a system must remain secure at all times and prevent a viewer from obtaining free previews for more than the maximum duration assigned to the particular service. The present invention provides a method and apparatus having the aforementioned and other advantages.

SUMMARY OF THE INVENTION

A method in accordance with the present invention provides video services to consumers via an information network. A video service is provided on a pay-per-view basis during a program epoch. A fixed period is defined during the program epoch when portions of the video service are available for viewing on a preview basis. A consumer is allowed to preview, without purchase, portions of the video service at any time during the fixed period for up to a maximum preview duration that is shorter than the fixed period. The maximum preview duration is preferably enforced in a cryptographically secure manner. In particular, a record can be maintained in a cryptographically secure manner to indicate the amount of unused preview time remaining for the consumer to view the video service during the fixed period. The fixed period during which portions of the video service are available for previewing, as well as data identifying whether a preview is available for a particular service, are also preferably maintained in a cryptographically secure manner.

In a preferred embodiment, the method of the invention enables a consumer to purchase the video service for viewing during the program epoch after previewing portions of the service. Also in the preferred embodiment, the program epoch is divided into a plurality of working key epochs (WKE's). A count of the WKE's is cryptographically authenticated. The authenticated count is used to implement (i.e., define and keep track of) said maximum preview duration.

The method can further comprise the steps of maintaining a record of services which the consumer has previewed during prior program epochs. The consumer is then prohibited from previewing a service during a current program epoch if the consumer has previewed any part of that service during a prior program epoch. This prevents a consumer from recording successive free previews in order to accumulate a full movie or other program for viewing. The record of services which the consumer has previewed during prior program epochs can be maintained in a cryptographically secure manner.

In an illustrated embodiment, up to N active records of previewable services can be maintained at a time. Each record comprises either a purchase record representing a previewable service that has been purchased by the consumer or a preview record representing a service that the consumer has selected for preview. The expiration of an active previewable service record is prevented until the program epoch for the service represented by that record is over. The expiration time is controlled by an expiration timer. Alternatively, the expiration can be prevented by establishing a fixed minimum time period (e.g., several hours) for each record. The fixed minimum record duration is longer than the longest service that has a free preview available.

The method of the present invention can also include the step of preventing the erasure of any preview record until the program epoch for the service represented thereby is over. In the illustrated embodiment, a preview record is converted to a purchase record upon purchase by the consumer of the service represented by the preview record. At the time of conversion, the purchase record is rendered irrevocable. In such an embodiment, the erasure of any preview record is prevented until the program epoch for the service represented thereby is over, except that a preview record can be erased by conversion to an irrevocable purchase record.

Whenever all N records of previewable services are active, additional previews are denied to the consumer. However, a consumer can still purchase a service, in which event one of the preview records will be overwritten with a purchase record. Preferably, the next to expire preview record will be the one that is overwritten. When a preview record is open, the consumer can be informed of how much unused preview time remains for the corresponding video service.

Apparatus in accordance with the present invention provides previews of services available for purchase via a communication network. First means process data received from the communication network. The data (i) identifies a service available for purchase, (ii) identifies a period of time (epoch) over which the service is provided, (iii) indicates whether a preview is available for the service, and (iv) provides information necessary to generate keys for enabling an authorized consumer to receive the service or a preview thereof. Second means, responsive to the first means when a preview is available for the service, are provided for keeping track of a fixed period during the epoch when previewing is permitted. A user interface cooperates with the first and second means for enabling a consumer to preview portions of the service at any time during the fixed period for up to a maximum preview duration that is shorter than the fixed period. The user interface also enables a consumer to purchase the service. Means are responsive to the first means for decrypting the service during a preview and after a purchase thereof.

The apparatus in accordance with the invention can further comprise means for enforcing the maximum preview duration in a cryptographically secure manner. The apparatus can maintain a record in a cryptographically secure manner to indicate the amount of unused preview time remaining for the consumer to view the service during the fixed period.

Means can be provided for maintaining up to N active records of previewable services at a time. Each record comprises either a purchase record representing a previewable service that has been purchased by the consumer or a preview record representing a service that the consumer has selected for preview. Means are provided for preventing the expiration of an active previewable service record until the program epoch for the service represented by that record is over. Means can further be provided for preventing the erasure of any preview record until the program epoch for the service represented thereby is over. In an illustrated embodiment, means are provided for converting a preview record to a purchase record upon purchase by the consumer of the service represented by the preview record. The purchase record provided by the converting means is rendered irrevocable. Except for possible conversion to an irrevocable purchase record, the erasure of any preview record is prevented until the program epoch for the service represented thereby is over.

The apparatus of the invention can further comprise means for denying any previews or previewable services to the consumer whenever all N previewable service records are active. Means can also be provided for informing the consumer of how much unused preview time remains for each service.

In an illustrated embodiment, the epoch over which the service is provided is divided into a plurality of working key epochs. A cryptographically authenticated count of the working key epochs is used to implement said maximum preview duration. Means are provided for further cryptographically authenticating at least the portion of the data that identifies whether a preview is available for said service, and the fixed period during which previewing is permitted.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of apparatus in accordance with the present invention;

FIG. **2** is a block diagram illustrating the decryption hierarchy used in accordance with the present invention;

FIG. **3** is a time line, illustrating different program epochs that occur over time;

FIGS. **4** and **4***a* provide a diagrammatic illustration of one program epoch, illustrating various boundaries contained therein and a sample of the working key epochs (WKE's) that occur during the program epoch;

FIG. **5** is a diagrammatic illustration of various preview/program records that are maintained in accordance with the invention;

FIG. **6** is the first part of a flowchart illustrating the authorization of anytime free previews in accordance with the present invention; and

FIG. **7** is a continuation of the flowchart of FIG. **6**.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** illustrates, in block diagram form, the decryption portion of a digital satellite or cable television receiver or the like. An encrypted service (e.g., a premium television service) is input to terminal **10**. By the time the bitstream comprising the service is input to terminal **10**, it has already been received and demodulated from the communication channel over which it is transmitted, using conventional techniques. The encrypted service is decrypted by a decryption processor **12** in order to provide a clear signal at output **16** of the decryption processor.

The decryption processor can utilize a conventional decryption scheme, such as that disclosed in Gilhousen, et al. U.S. Pat. No. 4,613,901 entitled "Signal Encryption and Distribution System for Controlling Scrambling and Selective Remote Descrambling of Television Signals," or Bennett et al. U.S. Pat. No. 4,864,615 entitled "Reproduction of Secure Keys By Using Distributed Key Generation Data," both incorporated herein by reference. The decryption processor requires working keys (WK) in order to decrypt the signals input thereto via terminal **10**. The working keys are generated by a secure processor **20** in response to control signals received via input/output (I/O) terminal **30**. Firmware for the secure processor is stored in read only memory (ROM) **24**. The secure processor is also provided with random access memory (RAM) **22** in a conventional manner. A secure portion of RAM **22** holds unit specific keys and/or seeds for use in decryption of a monthly key, as discussed in greater detail in connection with FIG. **2**.

A user interface **26** enables a viewer to select services for viewing on a television (TV) **28**. If a user is authorized to receive the selected service by subscription or individual purchase (e.g., pay per view), secure processor **20** will actuate switch **18** to couple the decrypted output **16** from decryption processor **12** to the TV **28** via user interface **26**. Otherwise, the user interface and TV will only receive the encrypted signal via line **14** and switch **18**.

A typical key hierarchy is illustrated in FIG. **2**. An encrypted program pre-key is input via terminal **40** to a decryption function **44** which also receives a monthly key via terminal **42**. The program pre-key is unique to each encrypted program offering (e.g., television program) that is available for decryption. The monthly key is changed on a periodic basis, e.g., once each month. The decryption function **44** decrypts the encrypted program pre-key to provide a program pre-key that is used as one input to a one-way function **48**. The other input to one way function **48** comprises various program attributes, including access requirements, for the corresponding program. The access requirements must be met in order to obtain authorization to view

the program. The program attributes are input via terminal **46**, and the one way function processes the program pre-key and program attributes to provide a program key. The program key output from one way function **48** is used as one input to another one way function **52** that also receives, via terminal **50**, an initialization vector (IV) representative of time. The processing of the initialization vector and program key by one way function **52** generates the working keys required by decryption processor **12** (FIG. **1**) to decrypt the service selected by an authorized user. A further description of the generation of the various keys, including working keys (provided in a "keystream"), can be found in the aforementioned Bennett, et al. patent.

FIG. **3** is a diagrammatic illustration of the initialization vector that is input to terminal **50** of one way function **52**. The initialization vector **60** commences at time=I and runs until time=J, which can be, for example, several weeks, at which time the count resets. During the time represented by the vector **60**, a plurality of program epochs (PE_1 through PE_n) occur. Each program epoch can be of a different length, and is associated with one program offering.

FIG. **4** is a diagrammatic illustration of one program epoch, generally designated **70**. The epoch starts at time **72** and ends at time **78**. Prior to the end of the epoch, there is an AFP boundary **74** and a program boundary **76**. The time between the start of the epoch **72** and the AFP boundary **74** is a fixed period during the program epoch when portions of the program are available for viewing on a preview basis. During this fixed period, the program can be previewed for a maximum AFP duration **82**. As indicated by arrows **84** and **86** in FIG. **4**, the AFP can be viewed at any time from the start of the epoch to the AFP boundary, but only for up to the maximum AFP duration "t" provided. In order to permit a viewer to view some part of the allowed free preview time, tune away, and then return to watch the remaining part, the maximum AFP duration **82** is maintained as a count of working keys which is decremented as the allowable AFP time is used up.

During a program epoch, working keys are generated for authorized subscribers that have purchased or, during a preview period, requested a preview of the program. The program epoch is divided into a plurality of working key epochs (WKE's) **80**, as illustrated in FIG. **4***a*. For example, the working key epochs may occur at a rate of eight WKE's per second, or at any other interval that is desirable for a given implementation of the system. The WKE's can provide a convenient means for maintaining the integrity of the AFP boundary **74**. In a preferred embodiment, the AFP boundary is the value of the WKE representing the boundary beyond which an anytime free preview is not allowed. This parameter is authenticated by including it in the program key generators. The computation and maintenance of the AFP boundary is discussed in greater detail below, in connection with FIGS. **6** and **7**.

The program boundary **76** is the point at which the program provided during the epoch is expected to end. The end of the epoch **78** may extend beyond the program boundary **76** to accommodate the possibility of a program running over its original expected length. For example, if a program is interrupted by a news bulletin, the program ending time may be extended. Similarly, since it is impossible to accurately predict the end of a sports event, it may be necessary to extend the program boundary within the program epoch to accommodate a game that runs into overtime.

In accordance with the present invention, no free previews are permitted after the AFP boundary **74**. Thus, during the portion of a program that runs between the AFP boundary **74** and the epoch end **78**, free previews can not be obtained. The reason for providing the AFP boundary is to defend against certain attacks by a pirate who attempts to use the AFP feature in order to obtain a program or service without proper payment. In particular, a pirate may attempt to change the time at which a program epoch ends in order to obtain free services. However, this will not help him steal successive anytime free previews, because the AFP boundary is an authenticated value beyond which free previews will not be available. Further, as explained in greater detail below, the present invention establishes "records" of previews and purchased programs, which are not allowed to expire prematurely in a way that would be helpful to a pirate.

In order to prevent the theft of services by taking advantage of the anytime free preview feature, the secure processor **20** (FIG. **1**) of the present invention securely regulates the duration of a program segment that may be viewed without purchase. In order to accomplish this, the anytime free preview duration is maintained in units of working key epochs. The secure processor **20** counts the number of free working keys generated. When the count reaches a limit established by the maximum AFP duration **82** (FIG. **4**), the authorization state is changed from "can buy or obtain a free preview" to "can buy only." The AFP duration is one of the program attributes that is included in the generation of the program key. Thus, it can not be altered without altering the program key itself, which would prevent the correct decryption of the program.

As mentioned above, the system of the present invention establishes a record for each program previewed or purchased. Once the user chooses to view an AFP, a "preview record" is created in the secure processor **20** to define the number of free working keys allowed, and to keep a real time counter to cause the record to expire when the event or program is over. The timer must continue to run whether or not the receiver is synchronized to a scrambled or encrypted waveform, so that records expire at the proper time. If an AFP record were to expire early, a second free viewing period could be taken. If the record expires late, no harm is done but the number of new free preview offerings is reduced during the existence of the record beyond the end of the program.

In accordance with the present invention, up to N multi-function records are maintained. Each record is either a "preview record" representing an anytime free preview selected by the user, a "purchase record" representing a program that the user has bought or an inactive (null) record. Also, in accordance with the present invention, it is not possible for a preview record for a given event to be erased before the event is over, except by a legitimate purchase of the event or another purchasable service, in which case the record is overwritten to provide a purchase record. Typically, a user will request a free preview, and then decide whether or not to purchase the event based on the free preview. If the event is not purchased, the preview record is maintained until the end of the event unless another service is purchased to overwrite it. If the user decides to purchase the event, then the preview record is converted to a purchase record.

Preventing the erasure of a preview record before the event is over is an essential feature of the present invention. If preview records were merely stored in a first-in first-out queue (FIFO), older records would be lost as new records are added. A user could then cumulatively watch more than the free preview limit by scanning through and watching one second of a number of programs to flush the queue, and then return to watch another free preview of the desired program.

This opportunity is precluded by the maintenance of each preview record for the entire event once the preview record is established.

Also in accordance with the invention, program purchases take precedence over free preview offerings. In a case where all N available preview/purchase records are active, and at least one record holds an AFP, the secure processor **20** will indicate the authorization state as "can buy." The reason for this is that even though all of the available preview/purchase records are in use, one of the active preview records can be replaced by a purchase record. Preferably, the preview record that is replaced by the purchase record will be the one that is closest to expiring.

It is also important to carefully control any opportunity for a user to erase a preview record, since the ability to erase such a record provides an opportunity for abuse. For example, a program that is "purchased" may have been created by a pirate in his own interest. Therefore, in the case where a program purchase (i.e., a purchase record) overwrites a preview record, the present invention provides various defenses. First, a purchase which overwrites a preview record involves a secure transfer of debit, in which the debit total of the user's decoder is increased by the program cost. The number of purchases made is also counted in a secure manner. Second, the purchase record itself remains in memory until the purchased event is over. In this manner, the record is not available for another anytime free preview until the termination of the purchased event.

If a program selected for purchase is the program defined by a preview record, then that record is simply converted to a purchase record and the record remains open. After a preview record has been activated, a subsequent purchase of that program will be irrevocable. In this manner, the record for the program can not be erased. As a further precaution, the secure processor **20** establishes a minimum expiration time for a purchase record. This minimum time can be, for example, on the order of one hour, and will frustrate potential attacks by a pirate that attempts to cause an early expiration of a purchase record.

Timing of program durations and anytime free preview periods is maintained by secure processor **20**. A real time program expiration counter is maintained in the secure processor for this purpose. Program durations and AFP periods can be given in units of working key epochs.

As indicated above, a set of multifunction records is maintained in the secure processor **20** to handle anytime free previews and purchased programs. A set of N such preview/program records is illustrated diagrammatically in FIG. **5**. The records **90**, **92**, **94**, **96** and **98** each include program attributes (including access requirements) for the particular program or event that the record pertains to. A preview record will also maintain a count of the time remaining (e.g., number of free working keys remaining) within the maximum AFP duration for watching a free preview. A purchase record is rendered irrevocable when established after a free preview.

The program attributes will comprise information such as the cost of the program, which access requirements (e.g., "tiers") a user must subscribe to in order to receive the program, whether an AFP is available for the program and if so how many free working keys are provided for the AFP, an initial free preview boundary if an initial free preview is available instead of or in addition to an anytime free preview, and various regional access information. Since the access requirements are authenticated by one way function **48**, as shown in FIG. **2**, none of these requirements can be altered without altering the program key that is used to generate the working keys for decrypting the program. If the program key used to decrypt differs from the one used to encrypt, decryption will fail. The inclusion of the maximum AFP duration (i.e., number of free WKs permitted) as an access requirement authenticates this parameter and prevents its alteration without invalidating the working keys.

Each preview/purchase record also includes a record valid flag, a purchase flag, an expiration timer count, and a portion of the program key used as a program identifier. The record valid flag can be, for example, a one bit flag that indicates whether the record is valid or not. This flag, when set, indicates that the record contents are valid. When the flag is clear, the record is currently undefined.

The purchase flag indicates that the record describes a purchase record instead of a preview record. The working key epoch count is disregarded if the purchase flag is set. The expiration timer counts in predefined units (e.g., 2.56 seconds) the time left in the program. Once the record is expired, the record valid flag is cleared.

The portion of the program key provided in the preview/purchase record comprises, e.g., five bytes of the clear program key and is used as a program identifier. The working key epoch count counts the number of working keys provided during the anytime free preview.

As part of the derivation of an authorization state, which is required to enable a user to view a program, the secure processor determines if a given program is viewable via an anytime free preview. If an AFP is offered for a particular program, but all of the N available preview/purchase records are in use (as indicated by their record valid flags), a free preview cannot be granted.

Although a preview record could be established each time a user tunes to a channel offering an AFP, such action is not preferred. The reason is that as a user successively tunes to different channels (an activity known as "channel surfing"), programs offering AFPs will be successively encountered and the N available records will be quickly used up. Thus, the user interface **26** (FIG. **1**) will offer the user the option to view an AFP if available, will offer the user the option to buy a program being previewed, will provide the user with an indication of how much free preview time is left for the program, and will handle cases where initial free preview (an offering of a preview for a limited duration at the very beginning of a program) and anytime free preview offerings interact. In a preferred embodiment, the user interface is provided via on screen displays on the user's television **28**. The generation of such on screen displays is well known in the art.

In general, an on screen display will be available when the secure processor determines that an AFP is available for an acquired program. The user interface will collect text messages defining the AFP option screen. If the user selects an AFP, the user interface reports this fact to the secure processor **20** and free access is granted for up to the maximum AFP duration. In an alternate embodiment, an AFP can be automatically granted when a sufficient time has elapsed after the user tunes to a particular service.

In order to handle possible conflicts between an initial free preview and an anytime free preview, it is preferable that several rules be enforced. First, if a program has been acquired during an initial free preview period (or during a preceding epoch), the fact that an AFP is offered shall be disregarded. If the user chooses not to purchase the program and the user encounters the same program at a later time

after the initial free period is over (i.e., after tuning away from the program and then back to the program), then an AFP may be offered. Second, a program purchased during the AFP period may never be cancelled. Once a purchase is made during an AFP period, the purchase is immediate and irrevocable.

FIGS. **6** and **7** illustrate, in flowchart form, the process by which anytime free previews are provided in accordance with the present invention. The routine commences at box **100**, and at box **102** a working key epoch message is acquired. The WKE message identifies the WKE count within the current program epoch. At box **104**, a program rekey message is acquired. As indicated in connection with the description of FIG. **2**, the program pre-key is required in order to generate the program key and ultimately the working keys for authorized users. At box **106**, the authorization state for the user is computed, in order to determine if the user is authorized to receive the program and any AFP provided for the program. If the user is authorized to receive the program, a determination is made at box **108** as to whether or not the user has indicated a desire to purchase the program. If so, a purchase record is created at box **110**. Upon creation of the purchase record, a truncated portion of the clear program key (output from one way function **48** of FIG. **2**) is stored at box **112**. The clear program key is used by one way function **52** (FIG. **2**) to derive the necessary working keys as indicated at box **114**.

While the working keys are generated, a determination is made at box **116** as to whether the program epoch has ended. If not, the derivation of working keys continues and the process loops between boxes **114** and **116** until the program epoch ends. Upon termination of the program epoch, the purchase record is deleted as indicated at box **118**. The routine then ends at box **120**.

If a program has not yet been purchased by an authorized user, the routine will proceed from box **108** to box **122** where a determination is made as to whether the program epoch has ended. If so, the routine ends at box **120**. If the program epoch has not ended, a determination is made at box **124** as to whether an anytime free preview is available. If not, the routine loops back to box **108**.

If an AFP is available for the program (as indicated, for example, by a non-zero AFP count or by a separate "AFP available" bit) a determination is made at box **126** as to whether the user has requested to watch a free preview. If not, the routine loops back to box **108**. If an AFP is requested, the routine passes to box **128** of FIG. **7**. At box **128**, a preview record is created. Then, at box **130** an AFP expiration counter (AEC) is initialized. At box **132**, the clear program key is stored together with the AFP count. The AFP count is decremented with each working key, and provides a record of the remaining time in the maximum AFP duration (i.e., the amount of time that the viewer has left to preview the program for free).

At box **134**, a working key is created and the AFP count is decremented. The program expiration time is then computed directly from the current working key epoch as indicated at box **136**. In this manner, the AFP record expiration is dynamically recalculated every working key. In particular, a variable M is computed where M=(AFP boundary-current WKE count). M is then converted to real time using simple scaling, and if the result is bigger than the AEC as determined at box **138**, the AEC is overwritten with the computed expiration time at box **140**. This will lengthen the AEC to prevent a pirate from attempting to shorten the AEC in order to extinguish a preview record and obtain an additional AFP for the program.

After the AEC is tested and if necessary, overwritten, a determination is made, at box **144**, as to whether the AFP maximum duration has expired (i.e., if the number of free working keys for the preview has been decremented to zero). If so, any further AFP for the program is deauthorized at box **152**. Otherwise, a determination is made at box **146** as to whether the AFP boundary has been passed. The AFP boundary is the working key epoch count representing the boundary beyond which an anytime free preview is not allowed. As indicated above, this parameter is authenticated by including it in the program key generators.

If the AFP boundary has been passed, any further AFP for the program is deauthorized at box **152**. Otherwise, a determination is made at box **148** as to whether the AFP has been terminated by the user. If not, the routine waits for the next working key epoch (box **149**) and then a new working key is created at box **134**. The routine then continues until either the AFP maximum duration has expired, the AFP boundary has been passed or the AFP is terminated by the user. Upon termination of the AFP by the user, the current AFP duration count is held as indicated at box **150** and nothing is done until the program is purchased, the program epoch ends, or an AFP is again requested. The AFP duration count will enable the user to reinitiate an anytime free preview during the program, and before the AFP boundary, until the maximum AFP duration has expired.

Upon holding the AFP duration count after an AFP is terminated by the user, or deauthorizing the AFP after the maximum AFP duration has expired or the AFP boundary has been passed, the routine of FIGS. **6** and **7** returns to box **108**. A user can then purchase the program or service unless the program epoch has ended.

In an alternate embodiment, the maintenance of the AFP expiration counter and computation of the expiration time from the WKE (boxes **130** and **136** to **140** of FIG. **7**) can be eliminated by simply setting a minimum preview record expiration time. For example, a preview record once established can be maintained for a minimum of two hours. This will secure the anytime free preview feature such that a pirate can not steal more than one AFP every two hours. If the minimum preview record expiration time is longer than the longest typical program epoch, then either this method or the method illustrated in FIG. **7** can be used to prevent the expiration of an active previewable service record until the program epoch for the service represented by that record is over.

It should now be appreciated that the present invention provides a free preview feature for services available for a fee over a communication network. A potential program purchaser is provided with the ability to view a limited number of minutes of a movie or other program for free, as an enticement to purchase the service. The present invention improves upon prior art implementations, where only the beginning portion of a movie could be viewed without charge. With the anytime free preview feature of the present invention, previewing is not limited to the beginning of a service. The duration of the free preview is variable and may be defined on a program by program basis by specifying, as a program attribute, a maximum AFP duration. The invention also enables a user to view a portion of an available free preview at one time, tune away, and then return to watch an additional portion of the free preview. The user can break the free preview into as many portions as desired, as long as the maximum AFP duration is not exceeded.

Although the invention has been described in connection with specific embodiments thereof, those skilled in the art

will appreciate that numerous adaptations and modifications may be made thereto without departing from the spirit and scope of the invention as set forth in the claims.

What is claimed is:

1. A method for providing video services to consumers via an information network, comprising the steps of:

providing a video service on a pay-per-view basis during a program epoch of a particular program of said video service;

providing a program pre-key;

using said program pre-key to determine a fixed period during said program epoch when portions of said video service are available for viewing on a preview basis;

allowing a consumer to preview, without purchase, portions of said video service at any time during said fixed period for up to a maximum preview duration that is shorter than said fixed period; and

enforcing said maximum preview duration in a cryptographically secure manner.

2. A method in accordance with claim 1 comprising the further step of:

enabling a consumer to purchase said video service for viewing during said program epoch after previewing portions thereof.

3. A method in accordance with claim 1 wherein said program epoch is divided into a plurality of working key epochs (WKE's), comprising the further steps of:

cryptographically authenticating a count of said WKE's; and

using the authenticated count to implement said maximum preview duration.

4. A method in accordance with claim 1 comprising the further step of:

maintaining a record to indicate the amount of unused preview time remaining for said consumer to view said video service during said fixed period;

wherein said record is maintained in a cryptographically secure manner.

5. A method in accordance with claim 1 comprising the further step of:

maintaining a record to indicate the amount of unused preview time remaining for said consumer to view said video service during said fixed period;

wherein said record is maintained in a cryptographically secure manner.

6. A method in accordance with claim 1 comprising the further steps of:

maintaining a record of services which said consumer has previewed during prior program epochs; and

prohibiting said consumer from previewing a service during a current program epoch if the consumer has previewed any part of that service during a prior program epoch.

7. A method in accordance with claim 6 wherein said record of services is maintained in a cryptographically secure manner.

8. A method in accordance with claim 1 comprising the further steps of:

maintaining up to N active records of previewable services at a time, each record comprising either a purchase record representing a previewable service that has been purchased by said consumer or a preview record representing a service that said consumer has selected for preview; and

preventing the expiration of an active previewable service record until the program epoch for the service represented by that record is over.

9. A method in accordance with claim 8 comprising the further step of:

preventing the erasure of any preview record until the program epoch for the service represented thereby is over.

10. A method in accordance with claim 8 comprising the further steps of:

converting a preview record to a purchase record upon purchase by the consumer of the service represented by the preview record; and

rendering the purchase record resulting from said converting step irrevocable.

11. A method in accordance with claim 10 comprising the further step of:

preventing the erasure of any preview record until the program epoch for the service represented thereby is over, except by conversion to an irrevocable purchase record.

12. A method in accordance with claim 8 comprising the further step of:

denying any additional previews to said consumer whenever all N previewable service records are active.

13. A method in accordance with claim 1 comprising the further step of:

informing said consumer of how much unused preview time remains for said video service.

14. A method in accordance with claim 1 wherein said fixed period is enforced in a cryptographically secure manner.

15. Apparatus for providing previews of services available for purchase via a communication network, comprising:

first means for processing data including a program pre-key received from said communication network, said data (i) identifying a service available for purchase, (ii) identifying an epoch over which said service is provided, (iii) indicating whether a preview is available for said service, and (iv) providing information necessary to generate keys for enabling an authorized consumer to receive said service or a preview thereof;

said program pre-key being used to determine a fixed period during said epoch when previewing is permitted;

second means responsive to said first means when a preview is available for said service for keeping track of said fixed period;

a user interface cooperating with said first and second means for enabling a consumer to preview portions of said service at any time during said fixed period for up to a maximum preview duration that is shorter than said fixed period, said user interface also enabling a consumer to purchase said service; and

means responsive to said first means for decrypting said service during a preview and after a purchase thereof.

16. Apparatus in accordance with claim 15 further comprising means for enforcing said maximum preview duration in a cryptographically secure manner.

17. Apparatus in accordance with claim 16 further comprising:

means for maintaining a record in a cryptographically secure manner to indicate the amount of unused preview time remaining for said consumer to view said service during said fixed period.

18. Apparatus in accordance with claim 15 further comprising:

means for maintaining a record in a cryptographically secure manner to indicate the amount of unused preview time remaining for said consumer to view said service during said fixed period.

19. Apparatus in accordance with claim 15 further comprising:

means for maintaining up to N records of active previewable services at a time, each record comprising either a purchase record representing a previewable service that has been purchased by said consumer or a preview record representing a service that said consumer has selected for preview; and

means for preventing the expiration of an active previewable service record until the program epoch for the service represented by that record is over.

20. Apparatus in accordance with claim 19 further comprising:

means for preventing the erasure of any preview record until the program epoch for the service represented thereby is over.

21. Apparatus in accordance with claim 19 further comprising:

means for converting a preview record to a purchase record upon purchase by the consumer of the service represented by the preview record; and

means for rendering the purchase record provided by said converting means irrevocable.

22. Apparatus in accordance with claim 21 further comprising:

means for preventing the erasure of any preview record until the program epoch for the service represented thereby is over, except by conversion to an irrevocable purchase record.

23. Apparatus in accordance with claim 19 further comprising:

means for denying any additional previews or previewable services to said consumer whenever all N previewable service records are active.

24. Apparatus in accordance with claim 15 wherein said user interface comprises:

means for informing said consumer of how much unused preview time remains for said service.

25. Apparatus in accordance with claim 15 wherein said epoch is divided into a plurality of working key epochs, a cryptographically authenticated count of which is used to implement said maximum preview duration.

26. Apparatus in accordance with claim 25 further comprising:

means for cryptographically authenticating at least the portion of said data that identifies whether a preview is available for said service.

27. Apparatus in accordance with claim 26 wherein said fixed period is enforced in a cryptographically secure manner.

28. Apparatus in accordance with claim 15 further comprising:

means for cryptographically authenticating at least the portion of said data that identifies whether a preview is available for said service.

29. Apparatus in accordance with claim 15 wherein said fixed period is enforced in a cryptographically secure manner.

* * * * *

United States Patent [19]

Bennett et al.

[11] **Patent Number: 4,864,615**

[45] **Date of Patent: Sep. 5, 1989**

[54] **REPRODUCTION OF SECURE KEYS BY USING DISTRIBUTED KEY GENERATION DATA**

[75] Inventors: **Christopher J. Bennett; Michael V. Harding,** both of San Diego; **Paul Moroney,** Cardiff-by-the-Sea, all of Calif.

[73] Assignee: **General Instrument Corporation,** New York, N.Y.

[21] Appl. No.: **200,111**

[22] Filed: **May 27, 1988**

[51] **Int. Cl.**[4] **H04L 9/02**

[52] **U.S. Cl.** **380/21;** 380/20; 380/47

[58] **Field of Search** 380/20, 21, 45, 47

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,613,901	9/1986	Gilhousen et al.	380/20
4,634,808	1/1987	Moerder	380/20
4,694,491	9/1987	Horne et al.	380/20
4,712,238	12/1987	Gilhousen et al.	380/20
4,736,422	4/1988	Mason	380/20
4,792,973	12/1988	Gilhousen et al.	380/20

OTHER PUBLICATIONS

Denning, "Cryptography and Data Security" Addison Wesley, 1982, pp. 14-16, 161-164, 169-171.

"Specification for Conditional Access Receivers", Draft NR-MSK Specification Vedlegg 4, Oct. 1987, pp. 40-44.

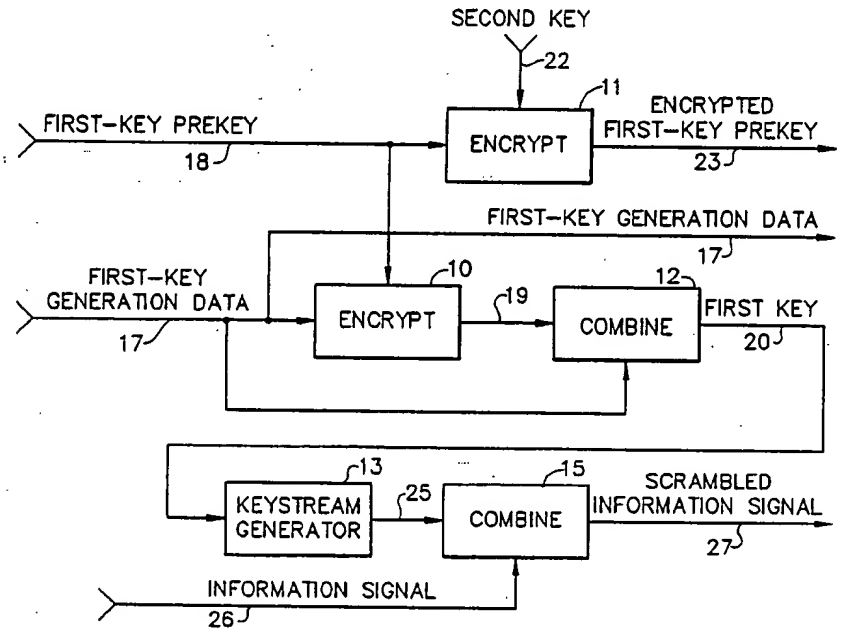
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—Edward W. Callan

[57] **ABSTRACT**

A key security system provides for the reproduction of secure keys by using distributed key generation data and a distributed encrypted prekey. The system encrypts program key generation data with a program key prekey in accordance with a first encryption algorithm to produce the program key; processes the program key to produce a keystream; and processes an information signal with the keystream to produce a scrambled information signal. The program key prekey is encrypted with a category key in accordance with a second encryption algorithm to produce an encrypted program key prekey. The scrambled information signal, the program key generation data and the encrypted program key prekey are distributed to descramblers. The descrambler within the key security system decrypts the distributed encrypted program key prekey with the category key in accordance with the second encryption algorithm to reproduce the program key prekey; encrypts the distributed program key generation data with the reproduced program key prekey in accordance with the first encryption algorithm to produce the program key; processes the reproduced program key to reproduce the keystream; and processes the distributed scrambled information signal with the reproduced keystream to descramble the distributed scrambled information signal. The key generation data incudes authorization data that must be processed by the authorization processor in the descrambler in order to enable the descrambler. The use of authorization data as key generation data protects the authorization data from spoofing attacks. When more data must be protected than a single operation of the encryption algorithm can support, then additional data blocks are protected by chaining the system, wherein the output from one stage forms part of the input to the next. The key generation data for the program key includes a sequence number securely associated with the category key to thereby "timelock" program key reproduction to the use of a current category key and thus prevent an attack based upon the use of an obsolete category key.

24 Claims, 9 Drawing Sheets



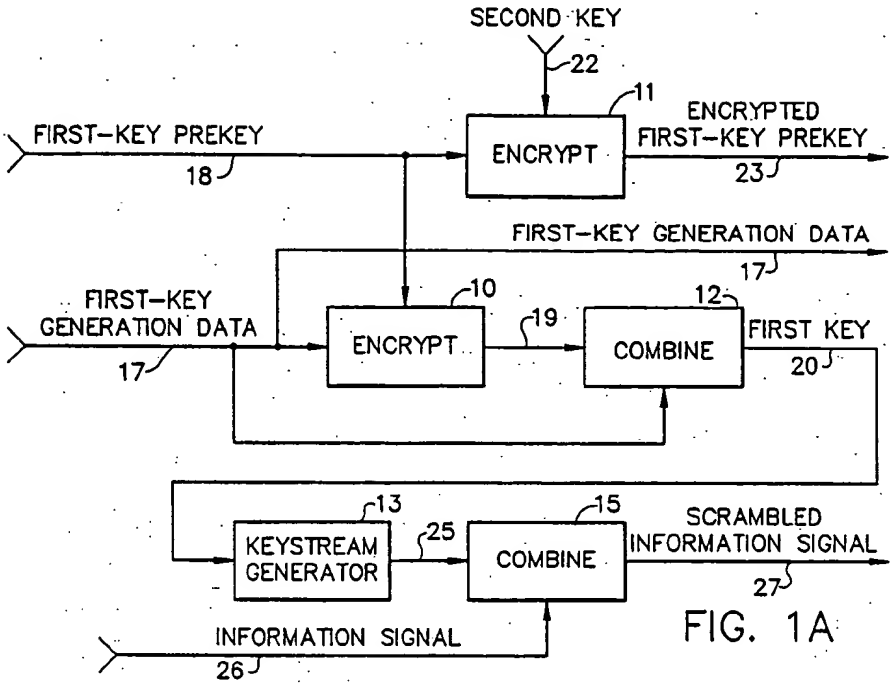

SECOND KEY
22
11
ENCRYPT
ENCRYPTED FIRST-KEY PREKEY
23
FIRST-KEY PREKEY
18
FIRST-KEY GENERATION DATA
17
10
ENCRYPT
19
12
COMBINE
FIRST KEY
20
FIRST-KEY GENERATION DATA
17
13
KEYSTREAM GENERATOR
25
15
COMBINE
SCRAMBLED INFORMATION SIGNAL
27
INFORMATION SIGNAL
26

FIG. 1A

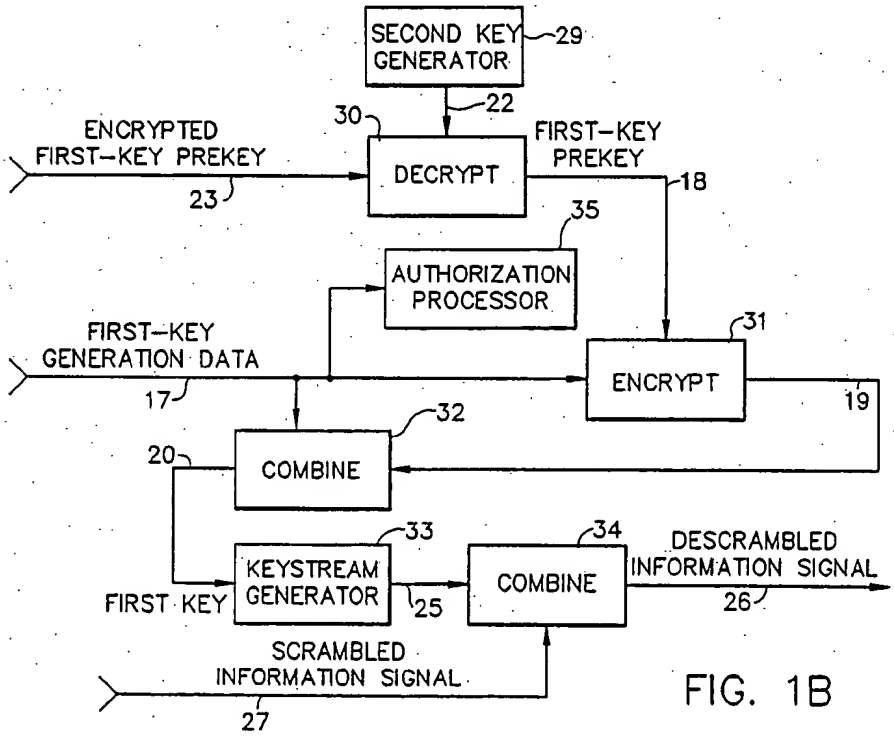

SECOND KEY GENERATOR
29
22
30
ENCRYPTED FIRST-KEY PREKEY
23
DECRYPT
FIRST-KEY PREKEY
18
35
AUTHORIZATION PROCESSOR
31
FIRST-KEY GENERATION DATA
17
ENCRYPT
19
32
20
COMBINE
33
34
KEYSTREAM GENERATOR
FIRST KEY
25
COMBINE
DESCRAMBLED INFORMATION SIGNAL
26
SCRAMBLED INFORMATION SIGNAL
27

FIG. 1B

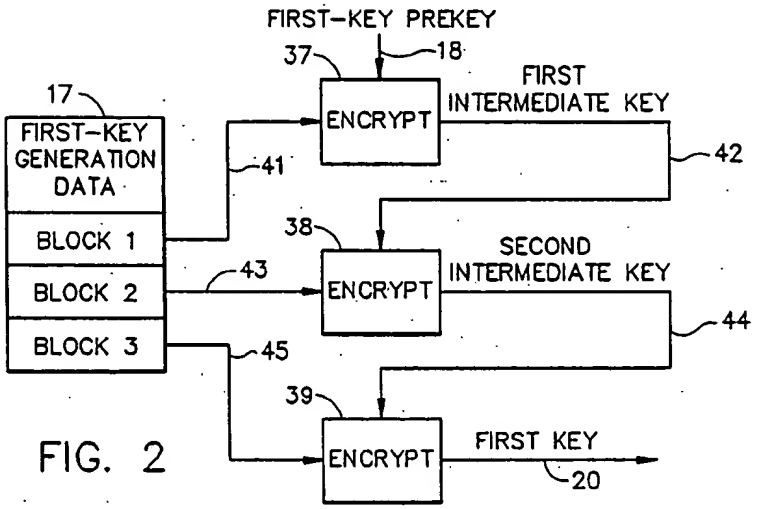

FIRST-KEY PREKEY
18
37
17
FIRST-KEY GENERATION DATA
BLOCK 1
BLOCK 2
BLOCK 3
41
ENCRYPT
FIRST INTERMEDIATE KEY
42
38
43
ENCRYPT
SECOND INTERMEDIATE KEY
44
45
39
ENCRYPT
FIRST KEY
20

FIG. 2

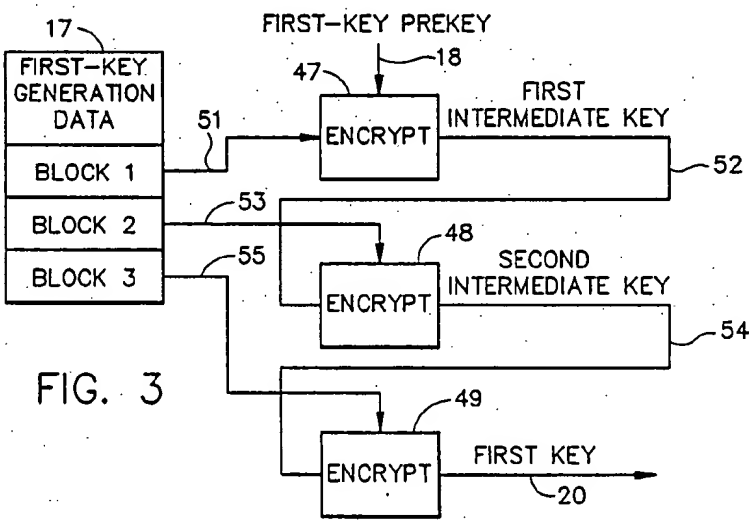

17
FIRST-KEY GENERATION DATA
BLOCK 1
BLOCK 2
BLOCK 3
FIRST-KEY PREKEY
18
47
51
ENCRYPT
FIRST INTERMEDIATE KEY
52
53
48
55
ENCRYPT
SECOND INTERMEDIATE KEY
54
49
ENCRYPT
FIRST KEY
20

FIG. 3

FIG. 4

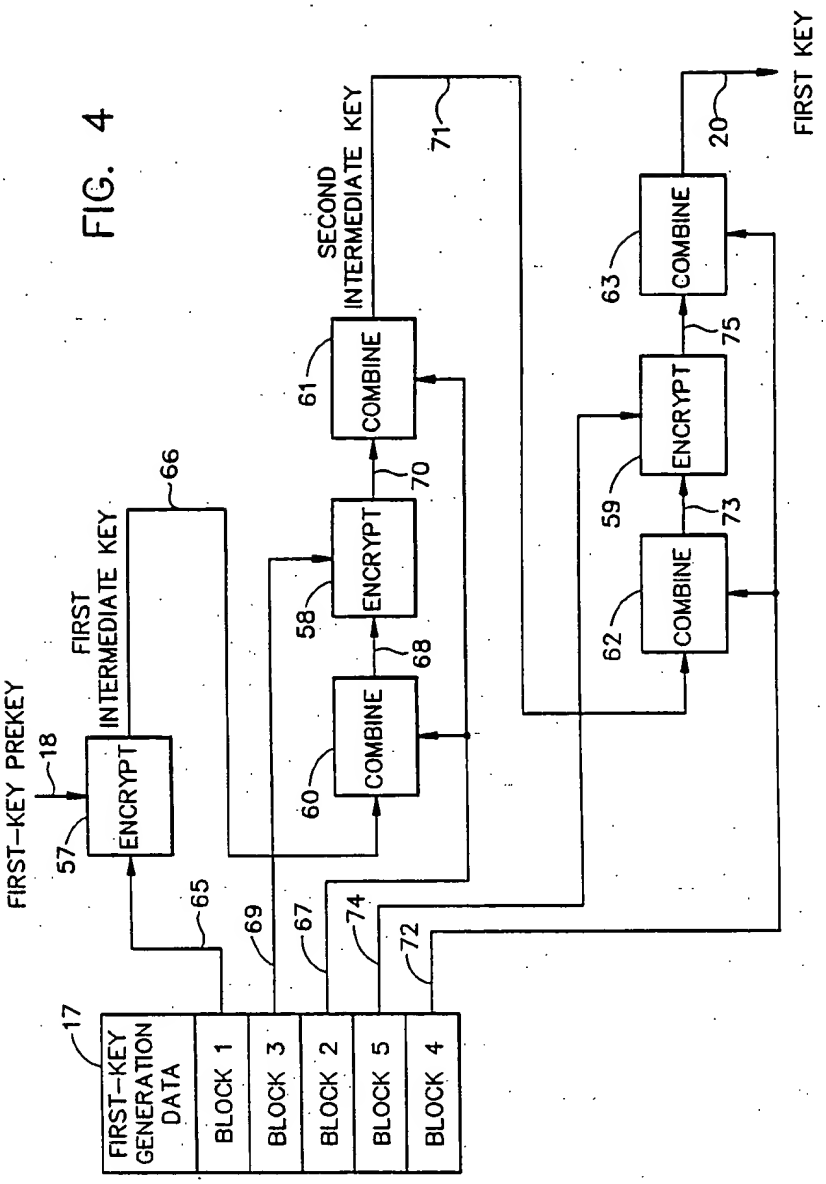
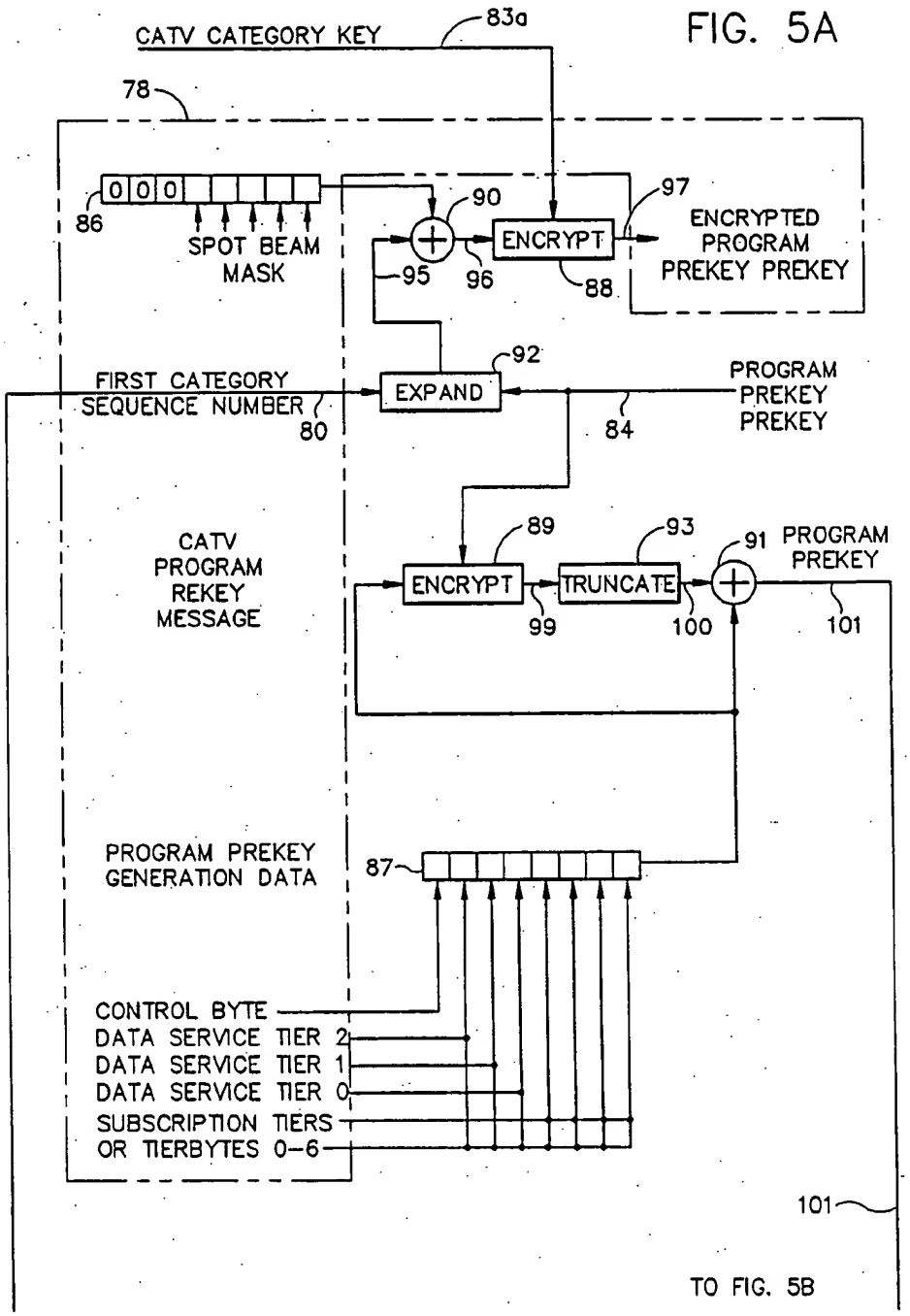

FIRST KEY
20
63
COMBINE
75
59
ENCRYPT
73
62
COMBINE
71
SECOND INTERMEDIATE KEY
61
COMBINE
70
58
ENCRYPT
68
60
COMBINE
66
FIRST INTERMEDIATE KEY
FIRST-KEY PREKEY
18
57
ENCRYPT
65
69
67
74
72
17
FIRST-KEY GENERATION DATA
BLOCK 1
BLOCK 3
BLOCK 2
BLOCK 5
BLOCK 4

FIG. 5A


CATV CATEGORY KEY
83a
78
0 0 0
86
SPOT BEAM MASK
90
ENCRYPT
97
ENCRYPTED PROGRAM PREKEY PREKEY
95
96
88
92
FIRST CATEGORY SEQUENCE NUMBER
80
EXPAND
PROGRAM PREKEY PREKEY
84
CATV PROGRAM REKEY MESSAGE
89
ENCRYPT
93
TRUNCATE
91
PROGRAM PREKEY
99
100
101
PROGRAM PREKEY GENERATION DATA
87
CONTROL BYTE
DATA SERVICE TIER 2
DATA SERVICE TIER 1
DATA SERVICE TIER 0
SUBSCRIPTION TIERS OR TIERBYTES 0-6
101
TO FIG. 5B

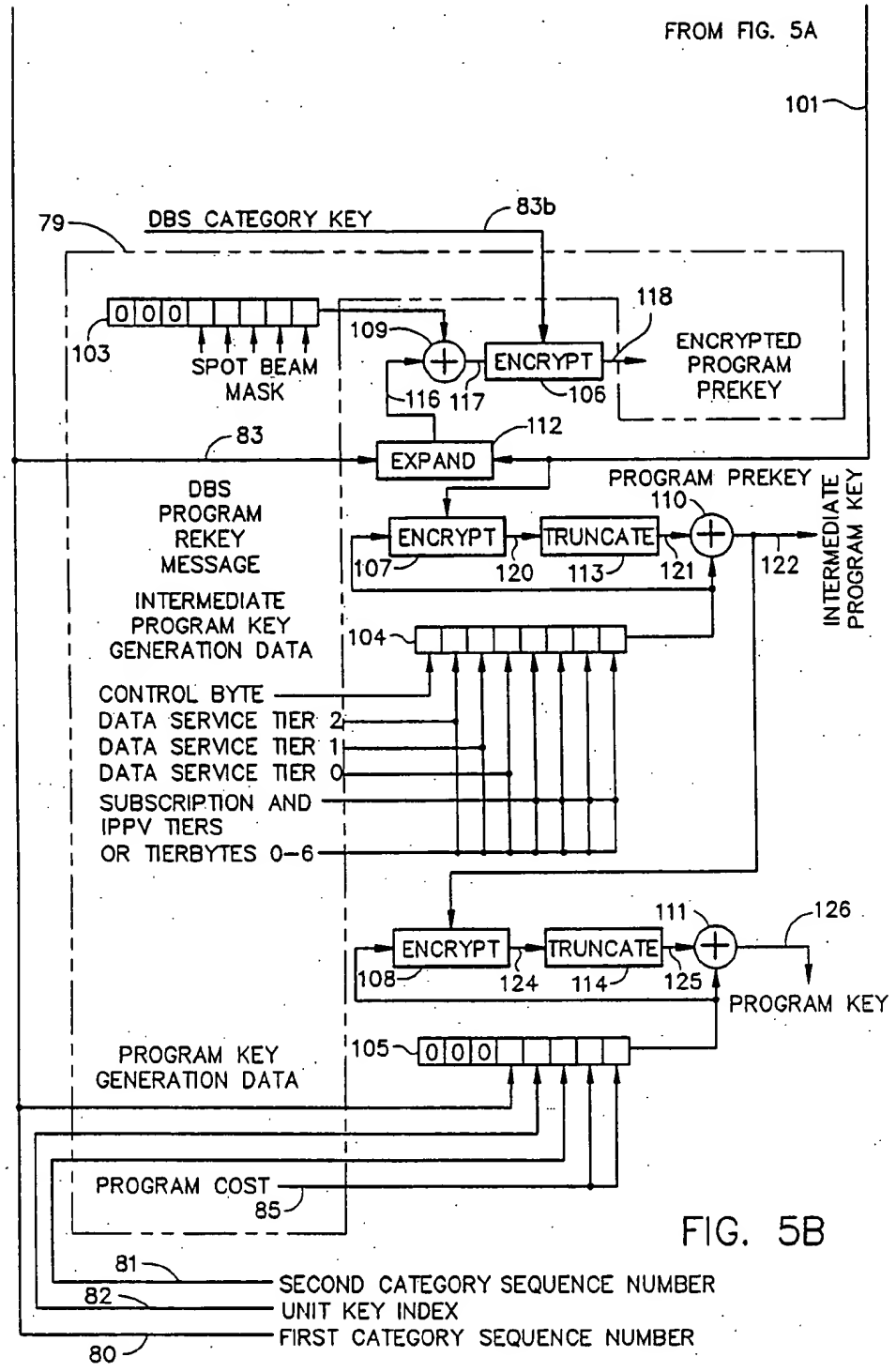

FROM FIG. 5A
101
79
DBS CATEGORY KEY
83b
0 0 0
103
SPOT BEAM MASK
109
ENCRYPT
118
ENCRYPTED PROGRAM PREKEY
116 117
106
83
EXPAND
112
DBS PROGRAM REKEY MESSAGE
PROGRAM PREKEY
110
ENCRYPT
TRUNCATE
107
120
113
121
122
INTERMEDIATE PROGRAM KEY
INTERMEDIATE PROGRAM KEY GENERATION DATA
104
CONTROL BYTE
DATA SERVICE TIER 2
DATA SERVICE TIER 1
DATA SERVICE TIER 0
SUBSCRIPTION AND IPPV TIERS OR TIERBYTES 0-6
111
126
ENCRYPT
TRUNCATE
108
124
114
125
PROGRAM KEY
105
0 0 0
PROGRAM KEY GENERATION DATA
PROGRAM COST
85
81
SECOND CATEGORY SEQUENCE NUMBER
82
UNIT KEY INDEX
FIRST CATEGORY SEQUENCE NUMBER
80

FIG. 5B

FIG. 6

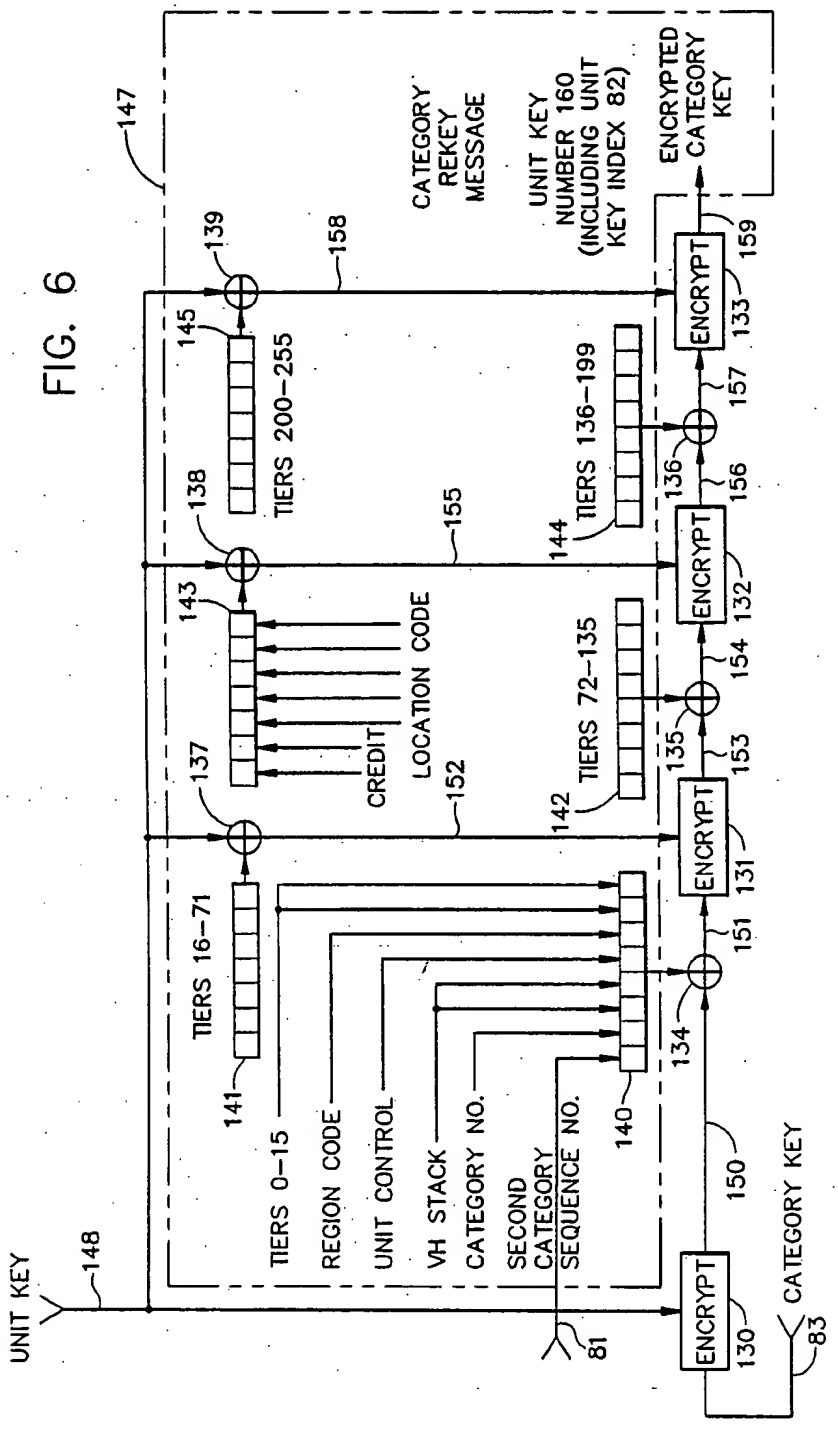
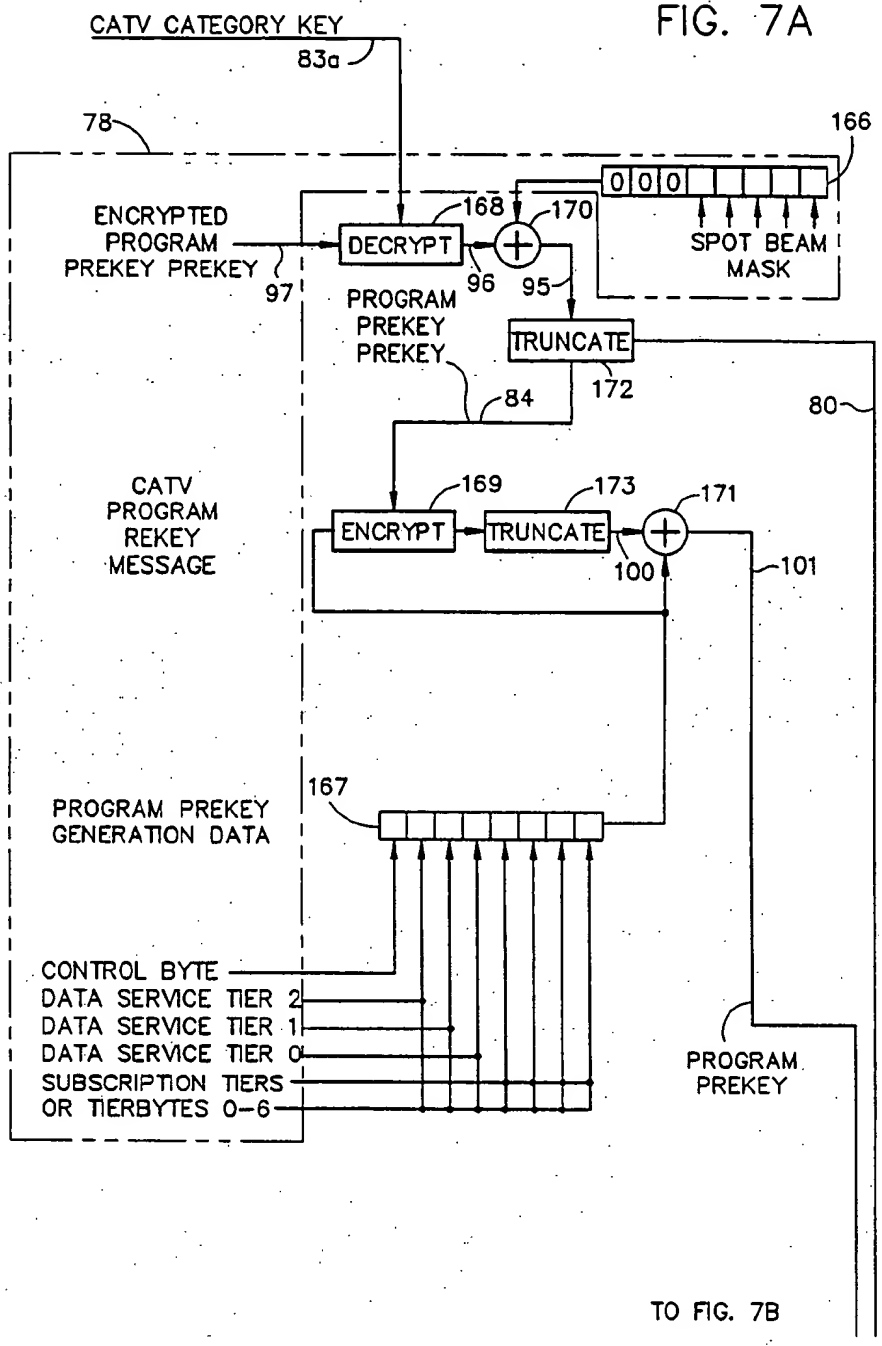

UNIT KEY
148
147
TIERS 0-15
REGION CODE
UNIT CONTROL
VH STACK
CATEGORY NO.
SECOND CATEGORY
SEQUENCE NO.
TIERS 16-71
TIERS 72-135
TIERS 136-199
TIERS 200-255
CREDIT
LOCATION CODE
CATEGORY REKEY MESSAGE
UNIT KEY NUMBER 160 (INCLUDING UNIT KEY INDEX 82)
ENCRYPTED CATEGORY KEY
CATEGORY KEY
ENCRYPT
81
83
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
150
151
152
153
154
155
156
157
158
159

FIG. 7A


CATV CATEGORY KEY
83a
78
166
0 0 0
ENCRYPTED PROGRAM PREKEY PREKEY
97
DECRYPT
168
170
96
95
SPOT BEAM MASK
PROGRAM PREKEY PREKEY
TRUNCATE
172
84
80
CATV PROGRAM REKEY MESSAGE
169
173
171
ENCRYPT
TRUNCATE
100
101
167
PROGRAM PREKEY GENERATION DATA
CONTROL BYTE
DATA SERVICE TIER 2
DATA SERVICE TIER 1
DATA SERVICE TIER 0
SUBSCRIPTION TIERS OR TIERBYTES 0-6
PROGRAM PREKEY
TO FIG. 7B

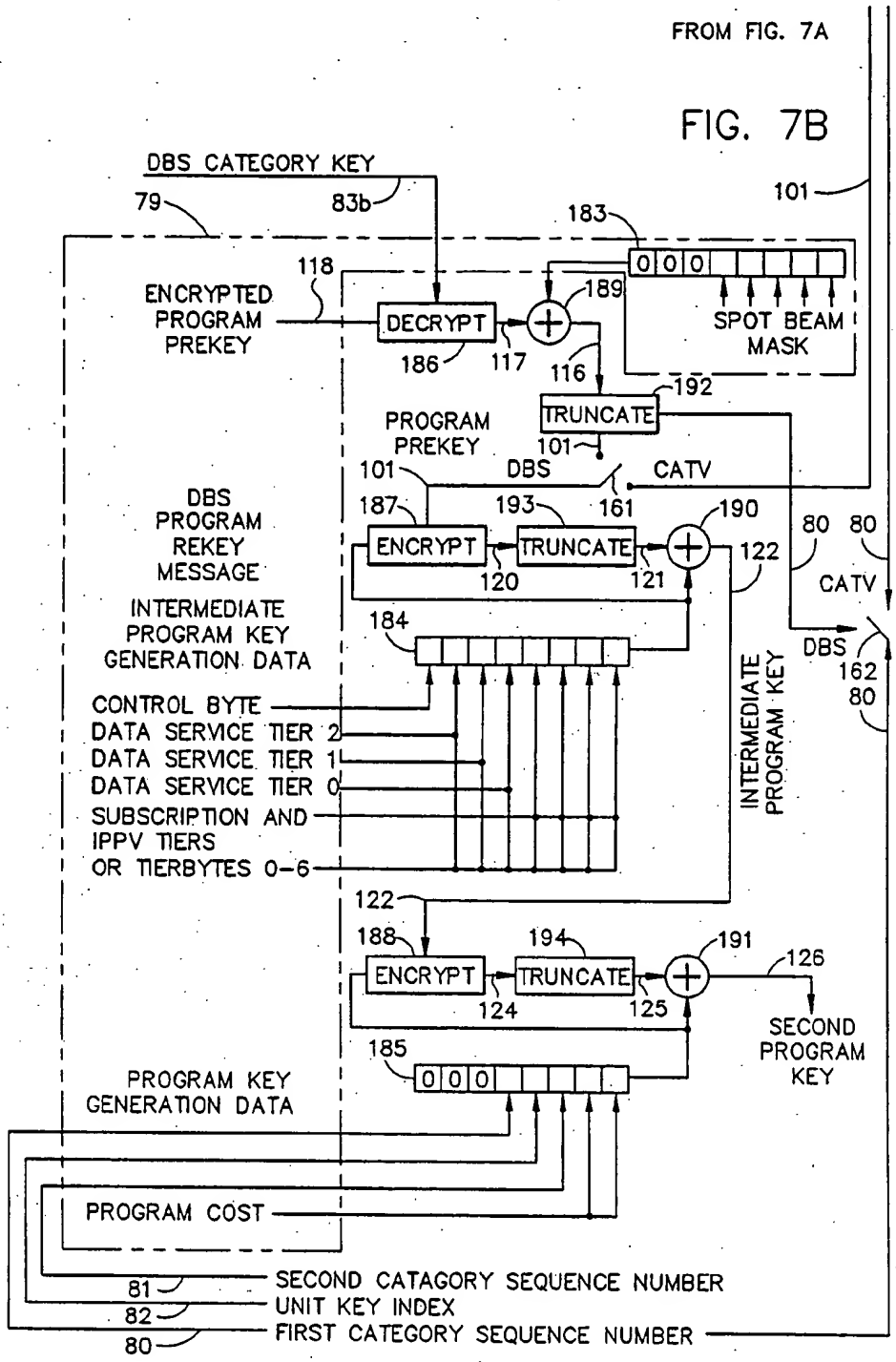
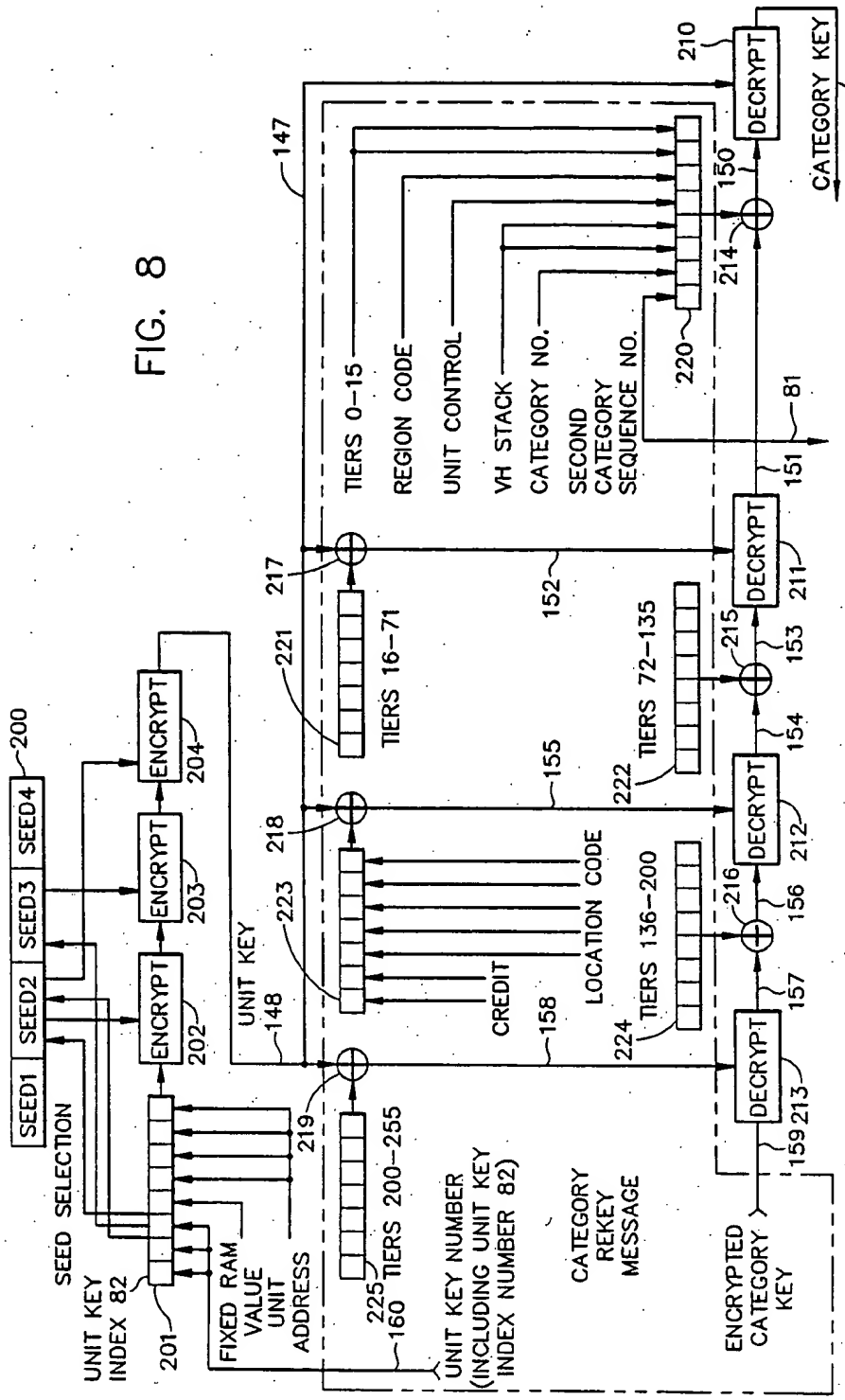

FROM FIG. 7A
DBS CATEGORY KEY
79
83b
101
183
0 0 0
118
ENCRYPTED PROGRAM PREKEY
DECRYPT
189
SPOT BEAM MASK
186
117
116
192
TRUNCATE
PROGRAM PREKEY
101
DBS
CATV
101
187
193
161
190
DBS PROGRAM REKEY MESSAGE
ENCRYPT
TRUNCATE
80 80
122
120
121
CATV
INTERMEDIATE PROGRAM KEY GENERATION DATA
184
DBS
162
80
CONTROL BYTE
DATA SERVICE TIER 2
DATA SERVICE TIER 1
DATA SERVICE TIER 0
SUBSCRIPTION AND IPPV TIERS OR TIERBYTES 0-6
INTERMEDIATE PROGRAM KEY
122
188
194
191
126
ENCRYPT
TRUNCATE
124
125
SECOND PROGRAM KEY
185
0 0 0
PROGRAM KEY GENERATION DATA
PROGRAM COST
81
SECOND CATAGORY SEQUENCE NUMBER
82
UNIT KEY INDEX
80
FIRST CATEGORY SEQUENCE NUMBER

FIG. 7B

FIG. 8


SEED1
SEED2
SEED3
SEED4
200
SEED SELECTION
UNIT KEY INDEX 82
201
ENCRYPT
202
ENCRYPT
203
ENCRYPT
204
FIXED RAM VALUE UNIT ADDRESS
UNIT KEY
148
219
TIERS 200-255
225
160
UNIT KEY NUMBER (INCLUDING UNIT KEY INDEX NUMBER 82)
217
218
TIERS 16-71
221
TIERS 136-200
224
CREDIT
158
LOCATION CODE
223
155
TIERS 72-135
222
152
TIERS 0-15
REGION CODE
UNIT CONTROL
VH STACK
CATEGORY NO.
SECOND CATEGORY SEQUENCE NO.
220
147
CATEGORY REKEY MESSAGE
ENCRYPTED CATEGORY KEY
DECRYPT
213
DECRYPT
212
DECRYPT
211
DECRYPT
210
159
157
156
154
153
151
150
214
216
215
81
CATEGORY KEY
83

REPRODUCTION OF SECURE KEYS BY USING DISTRIBUTED KEY GENERATION DATA

BACKGROUND OF THE INVENTION

The invention pertains to descrambling and decryption systems used in communications networks in which individual descramblers may be selectively authorized for access to the services provided by the network.

All such systems require the secure delivery of authorization data to the descrambler. Security of the signal carrying the services is obtained by a technique of ensuring that any tampering of the messages delivering the authorization data causes a violation of the authorization conditions required by the descrambler for providing successful access to the network. Examples of such technique are described below.

A classical "signature verification" technique, which is described by D. E. R. Denning "Cryptography and Data Security", Addison-Wesley, 1983, as applied to this type of communications system, requires the authorization message delivered to the descrambler to contain a data block which contains a known value of sufficient size encrypted under a key shared between the descrambler and the originator of the message. If the descrambler obtains the known value after decryption, then it accepts the message as describing the legitimate conditions for authorization.

A "data comparison" technique described in "Specification for Conditional Access Receivers", Draft NR-MSK Specification Vedlegg 4, Oct. 1987), requires an unknown value of a sufficiently large number of bits to be repeated twice in the encrypted portion of the authorization message. If the descrambler finds, after decryption, that the two blocks match then it accepts the message as describing the legitimate conditions for authorization.

A "selective delivery" technique described in U.S. Pat. No. 4,613,901 to Klein S. Gilhousen, Charles F. Newby, Jr. and Karl E. Moerder, utilizes a hierarchy of secret keys to provide access control. Each level of the hierarchy is associated with an address. If the descrambler does not possess one of the appropriate addresses, it does not receive the message destined for the address containing the secret key for that level of the hierarchy. Since the secret key at each level of the hierarchy is encrypted under the secret key of the next level, an attacker cannot substitute a message intended for a different address.

A "key modification" technique described in U.S. Pat. No. 4,712,238 to Klein S. Gilhousen, Jerrold A. Heller, Michael V. Harding and Robert D. Blakeney, is similar to the "selective delivery" technique, but delivers authorization data along with the secret keys. The authorization data is in the clear, but is used to alter the secret keys in such a way that any attempt to modify the clear data causes incorrect generation of the secret keys when the descrambler performs the decryption operation. Since the descrambler then possess the incorrect keys, it will not correctly decrypt the signal.

All these systems protect the authorization data against tampering based on modification to the authorization messages, where such modification is based solely on knowledge of the contents of the message and on the operation of the system. However, if an attacker is able to gain additional information about the keys in use by the descrambler, e.g. through theft of key lists, then the services are open to attacks known as "spoofing". In these attacks, the attacker intercepts the authorization message, decrypts certain portions of it, substitutes data desired by the attacker, and reencrypts the substituted message under the key known to be held by the descrambler. The resultant message is delivered to the descrambler, causing the descrambler to authorize incorrectly.

An object of the present invention is to render such attacks null and void, either immediately, or upon replacement of the compromised keys by the message originator. As a result of this, an attacker is forced either to compromise the descrambler hardware or to obtain the most basic keys, which cannot be changed because they are fixed inside the descrambler hardware.

SUMMARY OF THE INVENTION

The present invention provides a key security system and a descrambler for reproducing secure keys by using distributed key generation data and a distributed encrypted prekey.

The key security system of the present invention includes means for encrypting first-key generation data with a first-key prekey in accordance with a first encryption algorithm to produce a first key; means for processing the firs key to produce a keystream; means for processing an information signal with the keystream to produce a scrambled information signal; means for encrypting the first-key prekey with a second key in accordance with a second encryption algorithm to produce an encrypted first-key prekey; means for distributing the scrambled information signal, the first-key generation data and the encrypted first-key prekey; and a descrambler, including means for providing the second key; means for decrypting the distributed encrypted first-key prekey with the second key in accordance with the second encryption algorithm to reproduce the first-key prekey; means for encrypting the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the first key; means for processing the reproduced first key to reproduce the keystream; and means for processing the distributed scrambled information signal with the reproduced keystream to descramble the distributed scrambled information signal.

The present invention may be used to prevent, or guarantee termination of, such spoofing techniques as (1) substitution of pirate access specifications for the intended access specifications in the case when all access authorization must be possessed by the descrambler; (2) substitution of pirate access specification for the intended access specifications in the case when only part of the access authorization must be possessed by the descrambler; and (3) interception of a deauthorization message, thus causing the descrambler to remain authorized through the use of obsolete keys and/or authorization data.

The key generation data may include certain quantities related to the authorization process, and may be transmitted in the clear. These key generation data quantities may be transmitted in the same message as the prekey and/or may already be stored in the descrambler.

The contents of the key generation data and the prekey may be any data values that can be shared by all descramblers requiring the reproduced key. An example of such data, used in the preferred embodiment, is

the set of access tiers associated with a program in a subscription pay-TV system.

In the preferred embodiment, the messages carrying encrypted prekey and the key generation data are transmitted in the signal carrying the services of a subscription pay-TV system, but they may also be transmitted separately.

Once the descrambler has reproduced the prekey by decrypting the encrypted prekey it uses the reproduced prekey to process the key generation data to reproduce the key. Since the key reproduction is performed inside the descrambler, any attacker wishing to alter the key generation data to a desired value must also alter the prekey to obtain the same output data. Such an attack would also require breaking the encryption algorithm.

If the descrambler can be authorized by correctly setting only a small number of bits of the key generation data, then an attacker may be able to find a suitable pair of prekey and key generation data within a short time. To thwart such an attack the encryption process in producing the key is enhanced. In accordance with such enhanced encryption process, the key generation data is encrypted by the first key in accordance with the encryption algorithm to produce encrypted key generation data; and the encrypted key generation data is processed with the key generation data to produce the first key. In the face of such enhancement, an attacker would have to break the encryption algorithm regardless of the use of the key generation data or the prekey by the descrambler. This enhanced encryption process is used in the preferred embodiment.

If the prekey is delivered encrypted under a key provided in the descrambler, and the key generation data for the key derived from the prekey includes a sequence number securely associated with the stored key, then the descrambler can be configured so that it will not decrypt the prekey and generate the required key unless it possesses the correct key identified by the sequence number. This technique, referred to as "timelock", ensures that the descrambler always requires up-to-date keys, and prevents attacks based on the use of obsolete keys.

By repeated application of the basic techniques of the present invention, a chain of protection may be created whereby arbitrarily large blocks of authorization data are protected against spoofing attacks.

Such chains can be specified in such a way that a group of descramblers which does not require all the data in the chain can enter the chain at the earliest point which protects data applicable to that group of descramblers.

Also, if more data must be protected than a single operation of the encryption algorithm can support, then additional data blocks are protected by chaining the system, wherein the output from one stage forms part of the input to the next. In the first stage of the chain, the key generation number must be processed with a prekey. Subsequent stages may take several forms, such as described in the description of the preferred embodiments.

Chaining is also appropriate when two or more groups of descramblers must use the same key, but do not process the same key generation data. Each group of descramblers can be provided one encrypted prekey in a common message, and derive the data and keys used in the subsequent stages from key generation data acquired from messages referring to the later stages of the key reproduction process. The messages thus form a key generation chain. The entry point to the chain for each descrambler must be identified by a securely protected quantity.

A two-stage chain is used in program key generation in the preferred embodiment. Each block of key generation data represents the set of access tiers required for a given category (group) of descramblers; and the key generation chain is completed with a stage that uses sensitive program attributes as key generation data.

Another feature of the key security system of the present invention is that it may be used in a scrambled signal communication system that is compatible with certain existing digital descrambling systems, such as the system described in U.S. Pat. No. 4,712,238. In existing networks in which existing descramblers use a predetermined key hierarchy, such as that described in U.S. Pat. No. 4,712,238, it is possible to introduce a new family of descramblers into the network in a compatible fashion by sharing a program key generated by the final stage of the lowest level of the new key hierarchy which is different from the existing system. This can be done provided that the two systems share the same access control and keystream generation procedures below the point of linkage, and that the program key so generated by the new system (1) is valid for the same set of services in both systems; (2) is valid for the same period of time in both systems; and (3) has the same number of bits in both systems. Also it must be possible to deliver the program key produced in accordance with the present invention directly via a message in the presently existing system, preferably in an encrypted form.

Additional features of the present invention are described with reference to the description of the preferred embodiments.

BRIEF DESCRIPTION OF THE DRAWING

FIG. 1A is a block diagram of a preferred embodiment of the scrambling and key generation data and prekey processing portions of the key security system of the present invention.

FIG. 1B is a block diagram of a preferred embodiment of a descrambler used with the scrambling and key generation data and prekey processing portions of the key security system according to the present invention shown in FIG. 1A.

FIG. 2 illustrates one technique according to the present invention of using several blocks of descrambler authorization data as key generation data and thereby protecting such authorization data from such alteration as would enable unauthorized use of the descrambler.

FIG. 3 illustrates an alternative technique according to the present invention of using several blocks of descrambler authorization data as key generation data and thereby protecting such authorization data from such alteration as would enable unauthorized use of the descrambler.

FIG. 4 illustrates another alternative technique according to the present invention of using several blocks of descrambler authorization data as key generation data and thereby protecting such authorization data from such alteration as would enable unauthorized use of the descrambler.

FIG. 5, which is a combination of FIGS. 5A and 5B, is a block diagram of a preferred embodiment of a portion of a key security system according to the present invention that processes key generation data and a prekey for distribution to descramblers.

FIG. 6 is a block diagram of a further portion of the key security system of FIG. 5 in which a portion of the key generation data is processed to provide the key that is used to encrypt the prekey.

FIG. 7, which is a combination of FIGS. 7A and 7B, is a block diagram of a preferred embodiment of a portion of a descrambler according to the present invention that processes the distributed key generation data and encrypted prekey to provide the key used for descrambling the distributed scrambled information signal.

FIG. 8 is a block diagram of a further portion of the descrambler of FIG. 7 in which a portion of the key generation data is processed to provide the key that is used to decrypt the encrypted prekey.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to FIG. 1A, a preferred embodiment of the scrambling and key generation data and prekey processing portions of the key security system of the present invention includes a first encryption unit **10**, a second encryption unit **11**, a first signal combining unit **12**, a keystream generator **13** and a second signal combining unit **15**. The encryption units **10, 11** encrypt data in accordance with a predetermined encryption algorithm, such as the Data Encryption Standard (DES) algorithm. Other encryption algorithms also may be used. The encryption algorithm must be such that it is computationally infeasible to perform decryption without prior knowledge of the encryption key. The DES algorithm is an example of such an encryption algorithm. Both encryption units **10, 11** may be implemented in a single unit on a time-shared basis. The combining units **12, 15** process received signals in accordance with a predetermined processing scheme. In the preferred embodiment, the combining units **12, 15** are exclusive-OR (XOR) logic elements.

The first encryption unit **10** encrypts first-key generation data **17** with a first-key prekey **18** in accordance with a first encryption algorithm to produce encrypted first-key generation data **19**. The combining unit **12** processes the first-key generation data **17** with the encrypted first-key generation data **19** to produce a first key **20**.

The second encryption unit **11** encrypts the first-key prekey **18** with a second key **22** in accordance with a second encryption algorithm to produce an encrypted first-key prekey **23**. The second encryption algorithm may be identical to the first encryption algorithm, or different algorithms may be used.

The keystream generator **13** processes the first key **20** to produce a keystream **25**; and the combining unit **15** processes an information signal **26** with the keystream **25** to produce a scrambled information signal **27**.

The scrambled information signal **27**, the first-key generation data **17** and the encrypted first-key prekey **23** are distributed to descramblers, such as the descrambler shown in FIG. 1B.

Referring to FIG. 1B a preferred embodiment of a descrambler according to the present invention includes a second key generator **29**, a first decryption unit **30**, a third encryption unit **31**, a third combining unit **32**, a second keystream generator **33**, a fourth combining unit **34** and an authorization processor **35**. As in that portion of the key security system shown in FIG. 1A, the combining units **32, 34** process received signals in accordance with a predetermined processing scheme; and in the preferred embodiment, the combining units **32, 34** are XOR logic elements. Also, the decryption and encryption units **30, 31** respectively decrypt and encrypt data in accordance with a predetermined encryption algorithm, such as the DES algorithm. Other encryption algorithms also may be used; and both encryption units **30, 31** may be implemented in a single unit on a time-shared basis.

The second key generator **29** generates the second key **22**. In an alternative embodiment, the second key is stored in the descrambler instead of being generated in the descrambler. The first decryption unit **30** decrypts the distributed encrypted first-key prekey **23** with the second key **22** in accordance with the second encryption algorithm to reproduce the first-key prekey **18**.

The third encryption unit **31** encrypts the distributed first-key generation data **17** with the reproduced first-key prekey **18** in accordance with the first encryption algorithm to reproduce the encrypted first-key generation data **19**. The combining unit **32** processes the reproduced encrypted first-key generation data **19** with the distributed first-key generation data **17** to reproduce the first key **20**.

The keystream generator **33** processes the reproduced first key **20** to reproduce the keystream **25**; and the combining unit **34** processes the distributed scrambled information signal **27** with the reproduced keystream **25** to descramble the distributed scrambled information signal **27**.

The authorization processor processes the distributed key generation data **17** in order to enable the descrambler. Such authorization processing is of the nature described in U.S. Pat. No. 4,712,238, wherein authorization signals such as cost and credit signals and a program mask and authorization word are processed to enable a descrambler. By using such authorization signals as first-key generation data, the authorization signals are protected against alteration, since if they are altered the first-key generation data distributed to the descrambler is likewise altered, whereby the descrambler will not be able to reproduce the first key by using altered key generation data.

In some embodiments of the key security system of the present invention, the quantity of first-key generation data that must be processed by the authorization processor in the descrambler in order to enable the descrambler exceeds the encryption capacity of a single operation of the applicable encryption algorithm. In such a key security system, the key generation data is divided into data blocks and the first key is generated by a more complex series of encryption steps in order to protect all of the blocks of data. Examples of systems for performing such more complex processing are described with reference to FIGS. 2 through 4.

Referring to FIG. 2, a system for producing the first key in both the descrambler of FIG. 1B and that portion of the key security system shown in FIG. 1A includes a first encryption unit **37**, a second encryption unit **38** and a third encryption unit **39**. Each of the encryption units **37, 38, 39** respectively encrypts data in accordance with a predetermined encryption algorithm, such as the DES algorithm. Other encryption algorithms also may be used; and all three encryption units **37, 38, 39** may be implemented in a single unit on a time-shared basis.

The first encryption unit **37** encrypts a first block **41** of the first-key generation data **17** with the first-key prekey **18** in accordance with a first encryption algorithm to produce a first intermediate key **42**.

The second encryption unit 38 encrypts a second block 43 of the first-key generation data 17 with the first intermediate key 42 in accordance with a second encryption algorithm to produce a second intermediate key 44.

The third encryption unit 39 encrypts a third block 45 of the first-key generation data with the second intermediate key 44 in accordance with a third encryption algorithm to produce the first key 20.

The first, second and third encryption algorithms may be identical or different.

The number of encryption units included in the system of FIG. 2 is dependent upon the number of data blocks that are to be protected.

Each encryption unit 37, 38, 39 in the system of FIG. 2 preferably further includes the combining units shown in FIGS. 1A and 1B, wherein each block of key generation data is encrypted to produce an encrypted data block and also combined with the encrypted data block to produce the resultant key.

Referring to FIG. 3, another system for producing the first key in both the descrambler of FIG. 1B and that portion of the key security system shown in FIG. 1A includes a first encryption unit 47, a second encryption unit 48 and a third encryption unit 49. Each of the encryption units 47, 48, 49 respectively encrypts data in accordance with a predetermined encryption algorithm, such as the DES algorithm. Other encryption algorithms also may be used; and all three encryption units 47, 48, 49 may be implanted in a single unit on a time-shared basis.

The first encryption unit 47 encrypts a first block 51 of the first-key generation data 17 with the first-key prekey 18 in accordance with the first encryption algorithm to produce a first intermediate key 52.

The second encryption unit 48 encrypts the first intermediate key 52 with a second block 53 of the first-key generation data 17 in accordance with a second encryption algorithm to produce a second intermediate key 54.

The third encryption unit 49 encrypts the second intermediate key 54 with a third block 55 of the first-key generation data 17 in accordance with a third encryption algorithm to produce a first key 20.

The first, second and third encryption algorithms may be identical or different.

The number of encryption units included in the system of FIG. 3 is dependent upon the number of data blocks that are to be protected.

Each encryption unit 47, 48, 49 in the system of FIG. 3 preferably further includes the combining units shown in FIGS. 1A and 1B, wherein each block of key generation data is encrypted to produce an encrypted data block and also combined with the encrypted data block to produce the resultant key.

Referring to FIG. 4, still another system for producing the first key in both the descrambler of FIG. 1B and that portion of the key security system shown in FIG. 1A includes a first encryption unit 57, a second encryption unit 58, a third encryption unit 59, a first combining unit 60, a second combining unit 61, a third combining unit 62 and a fourth combining unit 63. Each of the encryption units 57, 58, 59 respectively encrypts data in accordance with a predetermined encryption algorithm, such as the DES algorithm. Other encryption algorithms also may be used; and all three encryption units 57, 58, 59 may be implemented in a single unit on a time-shared basis. The combining units 60, 61, 62, 63 preferably are XOR logic elements. Alternatively, other types of combining units may be used.

The first encryption unit 57 encrypting a first block 65 of the first-key generation data 17 with the first-key prekey 18 in accordance with the first encryption algorithm to produce a first intermediate key 66.

The first combining unit 60 processes a second block 67 of the first-key generation data 17 with the first intermediate key 66 to produce a preencrypted second block of data 68.

The second encryption unit 58 encrypts the preencrypted second block of data 68 with a third block 69 of the first-key generation data 17 in accordance with a second encryption algorithm to produce an encrypted second block of data 70.

The second combining unit 61 processess the encrypted second block of data 70 with the second block of data 67 to produce a second intermediate key 71.

The third combining unit 62 processes a fourth block 72 of the first-key generation data 17 with the second intermediate key 71 to produce a preencrypted fourth block of data 73.

The third encryption unit 59 encrypts the preencrypted fourth block of data 73 with a fifth block 74 of the first-key generation data 17 in accordance with a fourth encryption algorithm to produce an encrypted fourth block of data 75.

The fourth combining unit 63 processes the encrypted fourth block of data 75 with the fourth block of data 72 to produce the first key 20.

The first encryption unit 57 in the system of FIG. 4 preferably further includes the combining units shown in FIGS. 1A and 1B, wherein each block of key generation data is encrypted to produce an encrypted data block and also combined with the encrypted data block to produce the resultant key.

The first, second and third encryption algorithms may be identical or different.

The number of encryption and combining units included in the system of FIG. 4 is dependent upon the number of data blocks that are to be protected.

FIGS. 5 through 8 show a preferred embodiment of the security system of the present invention incorporated within a pay television system, such as described in U.S. Pat. No. 4,712,238.

The key hierarchy of the system generally follows that described in U.S. Pat. No. 4,613,901. However, in this embodiment, as described with reference in FIGS. 5 and 7, encrypted program prekeys and encrypted program prekey prekeys are distributed to the descramblers instead of encrypted program keys. In such patent the program keys are referred to as "channel" keys.

The output of this chain may be further modified if an impulse-purchasable program has a free preview portion. In this case, one bit of the output of the program key generation chain is complemented during the free preview portion of the program.

Referring to FIG. 5, the security system includes a CATV section for processing key generation data pertaining to CATV (cable television) broadcasts and a DBS section for processing key generation data pertaining to DBS (direct broadcast satellite) broadcasts. These sections are embodied in a first control computer. The first control computer generates a CATV program rekey message 78 (shown within dashed lines in FIG. 5A), a DBS program rekey message 79 (shown within dashed lines in FIG. 5B), a first category sequence number 80, a second category sequence number 81, a unit

key index 82, a CATV category key 83*a*, a DBS category key 83*b*, a program prekey prekey 84 and program cost data 85. The DBS category key 83*b* is different from the CATV category key 83*a*.

The CATV and DBS categories are distinguished functionally by the fact that they have different access requirement definitions. In order that the same program key is reproduced for both categories, the output of the CATV section is used as the initial prekey for the DBS section. All CATV descramblers, therefore, must process both the CATV and DBS information in order to derive the program key. However, only the CATV authorization data is processed by an authorization processor 35 to authorize a CATV descrambler. The concatenation of CATV and DBS program key production and reproduction chains is shown in the combination of FIGS. 5(A) and 5(*b*) and in the combination of FIGS 7(A) and 7(B). Additional categories could precede the CATV category in the chain if, for example, additional data services were to be provided to specialized data descramblers as well as to CATV and DBS descramblers. If the chain includes more than two stages, the key generation data for the additional stages includes a category number that is used as an address to select the program rekey message.

The output of this chain may be further modified if an impulse-purchasable program has a free preview portion. In this case, one bit of the output of the program key generation data chain is complemented during the free preview portion of the program.

The CATV section includes first and second data registers, 86, 87, first and second encryption units 88, 89, first and second XOR gates 90, 91, an expansion unit 92, and a truncation unit 93.

Program prekey generation data, is stored in the second register 87. This includes either a control byte, data service tiers bytes 0, 1 and 2, and four subscription tiers, as shown in FIG. 5A, or the control byte and seven tier bytes 0–6, as determined by the control byte. Each register section shown in the drawing contains one byte of data. The tier data indicates particular programming that may be descrambled on a subscription basis by CATV subscribers and on either a subscription or an impulse-pay-per-view (IPPV) basis by DBS subscribers.

The expansion unit 92 combines the program prekey prekey 84, which is seven bytes long, with the first category sequence number 80, which is one byte long, to produce an expanded eight-byte program prekey prekey 95. The first XOR gate 90 processes the expanded program prekey prekey 95 with spotbeam mask data stored in the first register 86 by modulo-2 addition to produce a preencrypted program prekey prekey 96. The first encryption unit 88 encrypts the preencrypted program prekey prekey 96 with the CATV category key 83*a* in accordance with a first encryption algorithm, such as the DES algorithm, to produce an encrypted program prekey prekey 97. Spotbeam mask data indicates geographical regions where descrambling of the broadcast television signal is authorized. The encrypted program prekey prekey 97 in included in the CATV program rekey message 78.

The second encryption unit 89 encrypts the program prekey generation data stored in the second register 87 with the program prekey prekey 84 in accordance with a second encryption algorithm to produce encrypted program key generation data 99. The truncation unit 93 reduces the length of the encrypted program generation data 99 by truncating the least significant data byte to produce truncated encrypted program key generation data 100, which is seven bytes long. The truncation unit 93 is required only if the encryption algorithm produces an 8-byte output signal upon being keyed with a 7-byte key. The second XOR gate 91 processes the seven-byte truncated encrypted program key generation data 100 with the seven bytes of program prekey generation data stored in the second register 87 other than the control byte by modulo-2 addition to produce a program prekey 101, which is forwarded to the DBS section (FIG. 5B). The first and second algorithms may be the same or different.

The DBS section includes first, second and third data registers 103, 104, 105, first, second and third encryption units 106, 107, 108, first, second and third XOR gates 109, 110, 111, an expansion unit 112, and first and second truncation units 113, 114.

Spotbeam mask data is stored in the first register 103.

Intermediate program key generation data is stored in the second register 104. This includes either a control byte, data service tiers bytes 0, 1 and 2, and four subscription tiers, as shown in FIG. 5A, or the control byte and seven tier bytes 0–6.

Program key generation data is stored in the third register 105. This includes the first category sequence number (one byte) 80, the second category sequence number (one byte) 81, the unit key index (one byte) 82, and two bytes of program cost data 85.

The expansion unit 112 combines the program prekey 101, which is seven bytes long, with the first category sequence number 80, which is one byte long, to produce an expanded eight-byte program prekey 116. The first XOR gate 109 processes the expanded program prekey 116 with spotbeam mask data stored in the first register 103 by modulo-2 addition to produce a preencrypted program prekey 117. The first encryption unit 106 encrypts the preencrypted program prekey 117 with the DBS category key 83*b* in accordance with a first encryption algorithm, such as the DES algorithm, to produce an encrypted program prekey 118. The encrypted program prekey 118 is included in the DBS program rekey message 79.

The second encryption unit 107 encrypts the first program key generation data stored in the second register 104 with the program prekey 101 in accordance with a second encryption algorithm to produce encrypted first program key generation data 120. The first truncation unit 113 reduces the length of the encrypted first program generation data 120 by truncating the least significant data byte to produce truncated encrypted first program key generation data 121, which is seven bytes long. The second XOR gate 110 processes the seven-byte truncated encrypted first program key generation data 121 with the seven bytes of program key generation data stored in the second register 104 other than the control byte by modulo-2 addition to produce an intermediate program key 122. The intermediate program key 122 may be encrypted by another category key and distributed to descramblers as an encrypted program key in accordance with a modified version of the prior art system described in U.S. Pat. No. 4,712,238. In the modified version of such prior art system, the descrambler thereof is modified by adding a stage that processes the program key reproduced therein in the same manner as the last stage of the descrambler shown in FIG. 7B herein processes the intermediate program key 122.

The third encryption unit 108 encrypts the second program key generation data stored in the second register 105 with the intermediate program key 122 in accordance with a third encryption algorithm to produce encrypted second program key generation data 124. The first, second and third algorithms may be the same or different. The second truncation unit 114 reduces the length of the encrypted second program generation data 124 by truncating the least significant data byte to produce truncated encrypted second program key generation data 125, which is seven bytes long. The third XOR gate 111 processes the seven-byte truncated encrypted second program key generation data 125 with the seven bytes of program key generation data stored in the second register 104 other than one of the permanent zero bytes by modulo-2 addition to produce a program key 126. The program key 126 is processed by the keystream generator 13 (FIG. 1A) to produce a keystream 25 for scrambling a television signal. In some embodiments, only the audio portion of the television signal is scrambled by combination with the keystream 25. The program key 126 may be encrypted by another category key and distributed to descramblers as an encrypted program key in accordance with the prior art system described in U.S. Pat. No. 4,712,238.

The different encryption units may be implemented by a single encryption unit on a time shared basis. Other processing units likewise may be implemented in single processing units on a time shared basis.

A portion of the key generation data is also processed in a second control computer at a signal distribution site to encrypt the category key 83 for distribution. Such processing is described with reference to FIG. 6.

The category key 83 also is used to authenticate certain unit-specific authorization data such as the descrambler unit's access tiers and impulse pay-per-view (IPPV) credit limit, by using repeated applications of the procedure described in U.S. Pat. No. 4,712,238.

In addition, the category key is used to authenticate the second category sequence number 81, which is used as a timelock on program key generation, and the category number, which identifies the descrambler's entry point in the program key generation chain.

For consumer descramblers supporting IPPV, the category key 83 is combined with the descrambler unit address and certain other data to create a unit-specific key which decrypts IPPV-related data items to create a secure authenticator, using the procedure described in U.S. Pat. No. 4,712,238.

The processing system of FIG. 6 is included in the second control computer. This processing system includes first, second, third and fourth encryption units 130, 131, 132, 133, first, second, third, fourth, fifth and sixth XOR gates 134, 135, 136, 137, 138, 139 and first, second, third, fourth, fifth and sixth registers 140, 141, 142, 143, 144, 145. Each of the registers stores eight bytes of data.

The second control computer generates a category rekey message including the information shown within the dashed lines 147, and a unit key 148 for each descrambler to which the category rekey message is addressed. The category key 83 and the second category sequence number 81 are received from the first control computer (FIG. 5). The category rekey message 147 is individually addressed to each descrambler. Lists of different unit keys 148 for the different descramblers, as based on a common unit key number 160, are provided to the second control computer. Different category rekey messages are provided for CATV and DBS subscribers.

The first register 140 stores the second category sequence number 81, a category number (one byte), a two byte view history (VH) stack, one byte of unit control data, one byte of region code data, and two tier data bytes for tiers 0–15.

The second register 141 stores seven tier data bytes for tiers 16–71.

The third register 142 stores eight tier data bytes for tiers 72–135.

The fourth register 143 stores two bytes of credit data pertaining to the descrambler to which the category rekey message 147 is addressed and five bytes of location code.

The fifth register 144 stores eight tier data bytes for tiers 136–199.

The sixth register 145 stores seven tier data bytes for tiers 200–255.

The first encryption unit 130 encrypts the category key 83 with the unit key 148 in accordance with a first encryption algorithm, such as the DES algorithm, to produce a first intermediate encrypted category key 150.

The first XOR gate 134 processes the first intermediate encrypted category key 150 with the data stored in the first register 140 by modulo-2 addition to produce a second intermediate encrypted category key 151.

The fourth XOR gate 137 processes the unit key 148 with the data stored in the second register 141 by modulo-2 addition to produce a first encrypted unit key 152.

The second encryption unit 131 encrypts the second intermediate encrypted category key 151 with the first encrypted unit key 152 in accordance with a second encryption algorithm to produce a third intermediate encrypted category key 153.

The second XOR gate 135 processes the third intermediate encrypted category key 153 with the data stored in the third register 142 by modulo-2 addition to produce a fourth intermediate encrypted category key 154.

The fifth XOR gate 138 processes the unit key 148 with the data stored in the fourth register 143 by modulo-2 addition to produce a second encrypted unit key 155.

The third encryption unit 133 encrypts the fourth intermediate encrypted category key 154 with the second encrypted unit key 155 in accordance with a third encryption algorithm to produce a fifth intermediate encrypted category key 156.

The third XOR gate 136 processes the fifth intermediate encrypted category key 156 with the data stored in the fifth register 144 by modulo-2 addition to produce a sixth intermediate encrypted category key 157.

The sixth XOR gate 139 processes the unit key 148 with the data stored in the sixth register 145 by modulo-2 addition to produce a third encrypted unit key 158.

The fourth encryption unit 133 encrypts the sixth intermediate encrypted category key 157 with the third encrypted unit key 158 in accordance with a fourth encryption algorithm to produce an encrypted category key 159. The encrypted category key 159 is included in each category rekey message 147. Each category rekey message 147 also includes a three-byte unit key number 160. The unit key number 160 includes the one-byte unit key index 82, which is common to all descramblers for a given program.

The first, second, third and fourth encryption algorithms may be the same or different. The first, second, third and fourth encryption units may be embodied in a single encryption unit on a time-shared bases.

The scrambled television program, the category rekey messages **147** and each program rekey message **78, 79** are distributed to the descramblers of the respective CATV and DBS broadcast systems.

FIGS. **7** and **8** illustrate a descrambler, which is included in a preferred embodiment of the security system of the present invention for descrambling television signals having their program keys secured by that portion of the security system described with reference to FIGS. **5** and **6**.

Referring to FIG. **7**, a descrambler included in a CATV system, makes use of a CATV section (FIG. 7A) for processing key generation data pertaining to CATV broadcasts and a DBS section (FIG. 7B) for processing key generation data pertaining to DBS broadcasts; whereas a descrambler included in a DBS system makes use of only the DBS section (FIG. 7B). The descrambler is adapted to process both the CATV rekey message **78** and the DBS program rekey message **79**. The descrambler includes first and second switches **161, 162**, which are placed in the DBS position when the descrambler is included in a DBS broadcast system, or placed in the CATV position when the descrambler is included in a CATV broadcast system. The positioning of the first and second switches **161, 161** is determined in accordance with a category number that is used as an address to select the CATV or DBS program rekey message.

The CATV section of the descrambler includes first and second data registers, **166, 167**, a decryption unit **168**, an encryption unit **169**, first and second XOR gates **170, 171**, and first and second truncation units **172, 173**.

Program prekey generation data, is stored in the second register **167**. This includes either a control byte, data service tiers bytes **0, 1** and **2**, and four subscription tiers, as shown in FIG. 7A, or the control byte and seven tier bytes **0–6**.

The decryption unit **168** decrypts the encrypted prekey prekey **97** with the CATV category key **83***a* in accordance with the first algorithm used by the encryption unit **88** in the first control computer (FIG. 5A) to provide reproduce the preencrypted program prekey prekey **96**.

The first XOR gate **170** processes the reproduced preencrypted program prekey prekey **96** with spotbeam mask data stored in the first register **166** by modulo-2 addition to reproduce the expanded program prekey prekey **95**. Since the reproduced expanded program prekey prekey **95** is eight bytes long, the first truncation unit **172** truncates one byte therefrom to reproduce the program prekey prekey **84**. The truncated byte is the first category sequence number **80**, which is provided via the switch **162** to the DBS section for use as part of the second key generation data for reproducing the second program key, as will be described below in relation to the reproduction of the second program key.

The encryption unit **169** encrypts the program prekey generation data stored in the second register **167** with the reproduced program prekey prekey **84** in accordance with the second encryption algorithm used by the second encryption unit **89** in the first control computer to reproduce the encrypted program key generation data **99**. The truncation unit **173** reduces the length of the reproduced encrypted program generation data **99** by truncating the least significant byte to reproduce the truncated encrypted program key generation data **100**, which is seven bytes long. The second XOR gate **171** processes the reproduced seven-byte truncated encrypted program prekey generation data **100** with the seven bytes of program key generation data stored in the second register **87** other than the control byte by modulo-2 addition to reproduce the program prekey **101**, which is forwarded to the DBS section (FIG. 7B).

The DBS section includes first, second and third data registers **183, 184, 185**, a decryption unit **186**, first and second encryption units **187, 188**, first, second and third XOR gates **189, 190, 191**, and first, second and third truncation units **192, 193, 194**.

Spotbeam mask data is stored in the first register **183**.

Intermediate program key generation data is stored in the second register **184**. This includes either a control byte, data service tiers bytes **0, 1** and **2**, and four subscription tiers, as shown in FIG. 7A, or the control byte and seven tier bytes **0–6**.

Program key generation data is stored in the third register **185**. This includes the first category sequence number (one byte) **80**, the second category sequence number (one byte) **81**, the unit key index (one byte) **82**, and two bytes of program cost data **85**. The second category sequence number **81** and the unit key index **82** are provided from the received category rekey message **147** to provide a timelock for reproduction of the program key.

The decryption unit **186** decrypts the encrypted prekey **118** with the DBS category key **83***b* in accordance with the first algorithm used by the encryption unit **106** in the first control computer (FIG. 5B) to provide reproduce the preencrypted program prekey **117**.

The first XOR gate **189** processes the reproduced preencrypted program prekey **117** with spotbeam mask data stored in the first register **183** by modulo-2 addition to reproduce the expanded program prekey **116**. Since the reproduced expanded program prekey **116** is eight bytes long, the first truncation unit **192** truncates one byte therefrom to reproduce the program prekey **101**. The truncated byte is the first category sequence number **80**, which is provided via the switch **162** to the register **185** for use as part of the second key generation data for reproducing the second program key, as will be described below.

The first encryption unit **187** encrypts the first program generation data stored in the second register **184** with the reproduced program prekey **101** in accordance with the second encryption algorithm used by the second encryption unit **107** in the first control computer to reproduce the encrypted first program key generation data **120**. The truncation unit **193** reduces the length of the reproduced encrypted first program generation data **120** by truncating the least significant byte to reproduce the truncated encrypted first program key generation data **121**, which is seven bytes long. The second XOR gate **190** processes the reproduced seven-byte truncated encrypted first program prekey generation data **121** with the seven bytes of program key generation data stored in the second register **184** other than the control byte by modulo-2 addition to reproduce the intermediate program key **122**.

The second decryption unit **188** decrypts the encrypted prekey **118** with the category key **83** in accordance with the first algorithm used by the encryption unit **106** in the first control computer (FIG.5B) to provide reproduce the preencrypted program prekey **117**.

The first XOR gate **189** processes the reproduced preencrypted program prekey **117** with spotbeam mask data stored in the first register **183** by modulo-2 addition to reproduce the expanded program prekey **116**. Since the reproduced expanded program prekey **116** is eight bytes long, the first truncation unit **192** truncates one byte therefrom to reproduce the program prekey **101**. The truncated byte is the first category sequence number **80**, which is provided via the switch **162** to the register **185** for use as part of the second key generation data for reproducing the second program key, as will be described below.

The first encryption unit **187** encrypts the first program generation data stored in the second register **184** with the reproduced program prekey **101** in accordance with the second encryption algorithm used by the second encryption unit **107** in the first control computer to reproduce the encrypted first program key generation data **120**. The truncation unit **193** reduces the length of the reproduced encrypted first program generation data **120** by truncating the least significant byte to reproduce the truncated encrypted first program key generation data **121**, which is seven bytes long. The second XOR gate **190** processes the reproduced seven-byte truncated encrypted first program prekey generation data **121** with the seven bytes of program key generation data stored in the second register **184** other than the control byte by modulo-2 addition to reproduce the intermediate program key **122**.

The second encryption unit **188** encrypts the second program key generation data stored in the third register **185** with the intermediate program key **122** in accordance with the third encryption algorithm used by the third encryption unit in the first control computer (FIG. 5B) to reproduce the encrypted second program key generation data **124**. The third truncation unit **194** reduces the length of the reproduced encrypted second program generation data **124** by truncating the least significant data byte to reproduce the truncated encrypted second program key generation data **125**, which is seven bytes long. The third XOR gate **191** processes the reproduced seven-byte truncated encrypted second program key generation data **125** with the seven bytes of program key generation data stored in the second register **185** other than one of the permanent zero bytes by modulo-2 addition to reproduce the program key **126**. The program key **126** is processed by the keystream generator **33** (FIG. 1B) to reproduce the keystream **25** for descrambling the scrambled television signal.

The section of the descrambler that processes the category rekey message to reproduce the category key **83** is described with reference to FIG. 8.

This processing section includes a key seed memory **200**, a unit key generation data register **201**, first, second and third encryption units **202, 203, 204**, first, second, third and fourth decryption units **210, 211, 212, 213**, first, second, third, fourth, fifth and sixth XOR gates **214, 215, 216, 217, 218, 219** and first, second, third, fourth, fifth and sixth registers **220, 221, 222, 223, 224, 225**. Each of the registers stores eight bytes of data. The different encryption units may be implemented by a single encryption unit on a time shared basis. Other processing units likewise may be implemented in single processing units on a time shared basis.

The first register **220** stores the second category sequence number **81**, which is also provided to the portion of the descrambler discussed in FIG. 7, a category number (one byte), a two byte view history (VH) stack, one byte of unit control data, one byte of region code data, and two tier data bytes for tiers **0–15**.

The second register **221** stores seven tier data bytes for tiers **16–71**.

The third register **222** stores eight tier data bytes for tiers **72–135**.

The fourth register **223** stores two bytes of credit data pertaining to the descrambler to which the category rekey message **147** is addressed and five bytes of location code.

The fifth register **224** stores eight tier data bytes for tiers **136–199**.

The sixth register **225** stores seven tier data bytes for tiers **200–255**.

The tier data, program cost data, and credit data are processed by the authorization processor **35** to determine whether the descrambler is to be enabled for descrambling the scrambled television signal, as described in the aforementioned U.S. Pat. No. 4,712,238.

The sixth XOR gate **219** processes the reproduced unit key **148** with the data stored in the sixth register **225** by modulo-2 addition to reproduce the third encrypted unit key **158**.

The fourth decryption unit **213** decrypts the encrypted category key **159** with the reproduced third encrypted unit key **158** is accordance with the fourth encryption algorithm used by the fourth encryption unit **143** in the second control computer (FIG. 6) to reproduce the sixth intermediate encrypted category key **157**.

The third XOR gate **216** processes the reproduced sixth intermediate encrypted category key **157** with the data stored in the fifth register **224** by modulo-2 addition to reproduce the fifth intermediate encrypted category key **156**.

The fifth XOR gate **218** processes the reproduced unit key **148** with the data stored in the fourth register **223** by modulo-2 addition to reproduce the second encrypted unit key **155**.

The third decryption unit **212** decrypts the reproduced fifth intermediate encrypted category key **156** with the reproduced second encrypted unit key **155** in accordance with the third encryption algorithm used by the third encryption unit **132** in the second control computer to reproduce the fourth intermediate encrypted category key **154**.

The second XOR gate **215** processes the reproduced fourth intermediate encrypted category key **154** with the data stored in the third register **222** to reproduce the third intermediate encrypted category key **153**.

The fourth XOR gate **217** processes the reproduced unit key **148** with the data stored in the second register **223** by modulo-2 addition to reproduce the first encrypted unit key **155**.

The second decryption unit **211** decrypts the reproduced third intermediate encrypted category key **153** with the reproduced first encrypted unit key **152** in accordance with the second encryption algorithm used by the second encryption unit **131** in the second control computer to reproduce the second intermediate encrypted category key **151**.

The first XOR gate **214** processes the reproduced second intermediate encrypted category key **151** with the data stored in the first register **220** to reproduce the first intermediate encrypted category key **150**.

The first decryption unit **210** decrypts the reproduced first intermediate encrypted category key **150** with the reproduced unit key **148** in accordance with

the first encryption algorithm used by the first encryption unit **130** in the first control computer to reproduce the category key **83**.

The unit key generation data register **201** stores a three byte unit key number **160**, which is included in the category rekey message **147**, a one-byte fixed RAM value, which is stored in an internal RAM, and an eight byte unit address. The key generation number includes the unit key index **82**, which is also included in the second program key generation data stored in the register **185** and processed to reproduce the program key **126**.

The first, second and third encryption units **202, 203, 204** encrypt the unit key generation data stored in the register **201** by using key seeds selected from the seed memory **200** in accordance with the contents of the unit key number **160** to reproduce the unit key **148** used to produce the encrypted category key **159** included in the category rekey message **147** addressed to the descrambler. Such reproduction of the unit key is in accordance with the teaching of U.S. Pat. No. 4,634,808 to Karl E. Moerder. One byte of the unit key number **160**, the unit key index **82**, is used as a timelock to couple unit keys with program keys as described with reference to FIGS. **5B** and **7B**.

The second category sequence number **81** and the unit key index **82** complete the timelocks linking the program key **126** to the category key **83** and unit keys **148**.

The first category sequence number **80** and the unit key index **82** complete the timelocks linking the program key **126** to the category key and the unit keys of the modified version of the prior art system described in U.S. Pat. No. 4,712,238.

In an alternative preferred embodiment, the invention is applied to the security concepts of shared addressing described in International Pat. Application No. PCT/GB84/00237, filed 2 July 1983. In such an alternative embodiment the unit key, generated as described above or by other means, is used to authenticate unit-specific data as described above, and to deliver a shared-address key, known to a small number of units which possess the same shared address. One byte of the shared address, the shared address index, may optionally be authenticated and used for timelock purposes. Category keys and the associated category number and sequence number are then delivered to all descramblers having a shared address with a single message, encrypted under the shared address key. The category sequence number must be authenticated using the shared address key so that it may be used for timelock purposes. The category key is used as before, but the final state of program key generation may also be extended to include the shared address index.

We claim:

1. A system, comprising

means for encrypting first-key generation data with a first-key prekey in accordance with a first encryption algorithm to produce a first key;

means for processing the first key to produce a keystream;

means for processing an information signal with the keystream to produce a scrambled information signal;

means for encrypting the first-key prekey with a second key in accordance with a second encryption algorithm to produce an encrypted first-key prekey;

means for distributing the scrambled information signal, the first-key generation data and the encrypted first-key prekey; and

a descrambler, including

means for providing the second key;

means for decrypting the distributed encrypted first-key prekey with the second key in accordance with the second encryption algorithm to reproduce the first-key prekey;

means for encrypting the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the first key;

means for processing the reproduced first key to reproduce the keystream; and

means for processing the distributed scrambled information signal with the reproduced keystream to descramble the distributed scrambled information signal.

2. A system according to claim **1**, wherein the means for producing the first key comprise

means for encrypting the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce encrypted first-key generation data; and

means for processing the first-key generation data with the encrypted first-key generation data to produce the first key; and wherein the means for reproducing the first key comprise

means for encrypting the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the encrypted first-key generation data; and

means for processing the distributed first-key generation data with the reproduced encrypted first-key generation data to reproduce the first key.

3. A system according to claim **2**, wherein the respective means for producing and reproducing the first key each comprises

means for truncating the encrypted first-key generation data; and

means for exclusive-ORing the truncated encrypted first-key generation data with the first-key generation data to produce the first key.

4. A system according to claim **1**,

wherein the first-key generation data includes a sequence number associated with the second key; and

wherein the means in the descrambler for providing the second key include means for processing the distributed sequence number to provide the second key.

5. A system according to claim **4**,

wherein the first-key generation data further includes a key index used for accessing data processed to provide the second key in the descrambler; and

wherein the means in the descrambler for providing the second key further include means for processing the distributed key index to provide the second key.

6. A system according to claim **1**,

wherein the first-key generation data includes a key index used for accessing data processed to provide the second key in the descrambler; and

wherein the means in the descrambler for providing the second key include means for processing the distributed key index to provide the second key.

7. A system according to claim 1,
wherein the first-key generation data includes a quantity of data that must be processed by an authorization processor in the descrambler in order to enable the descrambler, and wherein said quantity of data exceeds the encryption capacity of a single operation of said first encryption algorithm;
wherein the means for producing the first key comprise
means for encrypting a first block of the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce an intermediate key; and
means for encrypting a second block of the first-key generation data with the intermediate key in accordance with a third encryption algorithm to produce the first key;
wherein the means in the descrambler for reproducing the first key comprise
means for encrypting said first block of the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the intermediate key; and
means for encrypting said second block of the distributed first-key generation data with the reproduced intermediate key in accordance with a third encryption algorithm to reproduce the first key;
wherein the descrambler further includes an authorization processor for processing the distributed first-key generation data in order to enable the descrambler.

8. A system according to claim 1,
wherein the first-key generation data includes a quantity of data that must be processed by an authorization processor in the descrambler in order to enable the descrambler, and wherein said quantity of data exceeds the encryption capacity of a single operation of said first encryption algorithm;
wherein the means for producing the first key comprise
means for encrypting a first block of the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce a first intermediate key;
means for encrypting the first intermediate key with a second block of the first-key generation data in accordance with a third encryption algorithm to produce a second intermediate key;
means for encrypting the second intermediate key with a third block of the first-key generation data in accordance with a fourth encryption algorithm to produce the first key;
wherein the means in the descrambler for reproducing the first key comprise
means for encrypting the first block of the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the first intermediate key;
means for encrypting the reproduced first intermediate key with the second block of the distributed first-key generation data in accordance with the third encryption algorithm to reproduce the second intermediate key;
means for encrypting the reproduced second intermediate key with the third block of the distributed first-key generation data in accordance with the fourth encryption algorithm to reproduce the first key.
wherein the descrambler further includes an authorization processor for processing the distributed first-key generation data in order to enable the descrambler.

9. A system according to claim 1,
wherein the first-key generation data includes a quantity of data that must be processed by an authorization processor in the descrambler in order to enable the descrambler, and wherein said quantity of data exceeds the encryption capacity of a single operation of said first encryption algorithm;
wherein the means for producing the first key comprise
means for encrypting a first block of the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce a first intermediate key;
means for processing a second block of the first-key generation data with the first intermediate key to produce a preencrypted second block of data;
means for encrypting the preencrypted second block of data with a third block of the first-key generation data in accordance with a third encryption algorithm to produce an encrypted second block of data;
means for processing the encrypted second block of data with the second block of data to produce a second intermediate key;
means for processing a fourth block of the first-key generation data with the second intermediate key to produce a preencrypted fourth block of data;
means for encrypting the preencrypted fourth block of data with a fifth block of the first-key generation data in accordance with a fourth encryption algorithm to produce an encrypted fourth block of data; and
means for processing the encrypted fourth block of data with the fourth block of data to produce the first key;
wherein the means in the descrambler for reproducing the first key comprise
means for encrypting the first block of the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the first intermediate key;
means for processing the second block of the distributed first-key generation data with the reproduced first intermediate key to reproduce the preencrypted second block of data;
means for encrypting the reproduced preencrypted second block of data with the third block of the distributed first-key generation data in accordance with the third encryption algorithm to reproduce the encrypted second block of data;
means for processing the reproduced encrypted second block of data with the second block of data to reproduce a second intermediate key;
means for processing the fourth block of the distributed first-key generation data with the reproduced second intermediate key to reproduce the preencrypted fourth block of data;

means for encrypting the reproduced preencrypted fourth block of data with the fifth block of the distributed first-key generation data in accordance with the fourth encryption algorithm to reproduce the encrypted fourth block of data; and

means for processing the reproduced encrypted fourth block of data with the fourth block of data to reproduce the first key;

wherein the descrambler further includes an authorization processor for processing the distributed first-key generation data in order to enable the descrambler.

10. A system according to claim 1,

wherein the means for processing the first key to produce the keystream, comprise

means for encrypting third-key generation data with the first key in accordance with a third encryption algorithm to produce a third key; and

means for processing the third key to produce the keystream;

wherein the distributing means further distribute the third key generation data; and

wherein the means in the descrambler for processing the reproduced first key to reproduce the keystream, comprise

means for encrypting the distributed third key generation data with the reproduced first key in accordance with the third encryption algorithm to reproduce the third key; and

means for processing the reproduced third key to reproduce the keystream.

11. A system according to claim 1, further comprising

means for encrypting third key generation data with the first key in accordance with a third encryption algorithm to produce a third key;

means for processing the third key to produce the keystream;

wherein the distributing means further distribute the third key generation data; and

a second descrambler, including

means for providing the second key;

means for decrypting the distributed encrypted first-key prekey with the second key in accordance with the second encryption algorithm to reproduce the first-key prekey;

means for encrypting the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the first key;

means for encrypting the distributed third key generation data with the reproduced first key in accordance with the third encryption algorithm to reproduce the third key;

means for processing the reproduced third key to reproduce the keystream; and

means for processing the distributed scrambled information signal with the reproduced keystream to descramble the distributed scrambled information signal.

12. A system according to claim 1, further comprising

means for encrypting the first key generation data with the second key in accordance with a third encryption algorithm to produce an encrypted first key;

wherein the distributing means further distribute the encrypted first key; and

a second descrambler, including

means for providing the second key;

means for decrypting the distributed encrypted first key with the second key in accordance with the third encryption algorithm to reproduce the first key;

means for processing the reproduced first key to reproduce the keystream; and

means for processing the distributed scrambled information signal with the reproduced keystream to descramble the distributed scrambled information signal.

13. A system according to claim 1, further comprising

means for encrypting first-key prekey generation data with a first-key prekey prekey in accordance with a third encryption algorithm to produce the first-key prekey;

means for encrypting the first-key prekey prekey with the second key in accordance with a fourth encryption algorithm to produce an encrypted first-key prekey prekey;

wherein the distributing means further distribute the encrypted first-key prekey prekey, the first-key prekey generation data and a descrambler category identification number;

wherein the descrambler further comprises

means for decrypting the distributed encrypted first-key prekey prekey with the second key in accordance with the fourth encryption algorithm to reproduce the first-key prekey prekey;

means for encrypting the distributed first-key prekey generation data with the reproduced first-key prekey prekey in accordance with the third encryption algorithm to reproduce the first-key prekey; and

switching means responsive to the distributed descrambler category identification number for causing the first-key prekey that is used to encrypt the distributed first-key generation data to be reproduced by either (a) decrypting the distributed encrypted first-key prekey with the second key in accordance with the second algorithm or (b) decrypting the distributed encrypted first-key prekey prekey with the second key in accordance with the fourth algorithm to reproduce the first-key prekey prekey and encrypting the distributed first-key prekey generation data with the reproduced first-key prekey prekey in accordance with the third algorithm.

14. A descrambler for descrambling a scrambled information signal produced by a system that encrypts first-key generation data with a first-key prekey in accordance with a first encryption algorithm to produce a first key; processes the first key to produce a keystream; processes the information signal with the keystream to produce a scrambled information signal; encrypts the first-key prekey with a second key in accordance with a second encryption algorithm to produce an encrypted first-key prekey; and distributes the scrambled information signal, the first-key generation data and the encrypted first-key prekey, the descrambler comprising

means for providing the second key;

means for decrypting the distributed encrypted first-key prekey with the second key in accordance with the second encryption algorithm to reproduce the first-key prekey;

means for encrypting the distributed first-key generation data with the reproduced first-key prekey in

accordance with the first encryption algorithm to reproduce the first key;

means for processing the reproduced first key to reproduce the keystream; and

means for processing the distributed scrambled information signal with the reproduced keystream to descramble the distributed scrambled information signal.

15. A descrambler according to claim 14 for descrambling an information signal scrambled by a said system in which the first key is produced by encrypting the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce encrypted first key-generation data; and processing the first key generation data with the encrypted first-key generation data to produce the first key, wherein the means for reproducing the first key comprise

means for encrypting the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the encrypted first-key generation data; and

means for processing the distributed first-key generation data with the reproduced encrypted first-key generation data to reproduce the first key.

16. A descrambler according to claim 15 for descrambling an information signal scrambled by a said system in which the first key is further produced by truncating the encrypted first-key generation data and exclusive-ORing the truncated first-key generation data with the first key generation data to produce the first key, wherein the means for reproducing the first key comprises

means for truncating the encrypted first-key generation data; and

means for exclusive-ORing the truncated encrypted first-key generation data with the distributed first-key generations data to reproduce the first key.

17. A descrambler according to claim 14 for descrambling an information signal scrambled by a said system, wherein the first-key generation data includes a quantity of data that must be processed by an authorization processor in the descrambler in order to enable the descrambler, and wherein said quantity of data exceeds the encryption capacity of a single operation of said first encryption algorithm; and in which system the first key is produced by encrypting a first block of the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce an intermediate key; and encrypting a second block of the first-key generation data with the intermediate key in accordance with a third encryption algorithm to produce the first key,

wherein the means in the descrambler for reproducing the first key comprise

means for encrypting said first block of the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the intermediate key; and

means for encrypting said second block of the distributed first-key generation data with the reproduced intermediate key in accordance with a third encryption algorithm to reproduce the first key;

wherein the descrambler further includes an authorization processor for processing the distributed first-key generation data in order to enable the descrambler.

18. A descrambler according to claim 14 for descrambling an information signal scrambled by a said system, wherein the first-key generation data includes a quantity of data that must be processed by an authorization processor in the descrambler in order to enable the descrambler, and wherein said quantity of data exceeds the encryption capacity of a single operation of said first encryption algorithm; and in which system the first key is produced by encrypting a first block of the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce a first intermediate key; encrypting the first intermediate key with a second block of the first-key generation data in accordance with a third encryption algorithm to produce a second intermediate key; encrypting the second intermediate key with a third block of the first-key generation data in accordance with a fourth encryption algorithm to produce the first key,

wherein the means in the descrambler for reproducing the first key comprise

means for encrypting the first block of the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the first intermediate key;

means for encrypting the reproduced first intermediate key with the second block of the distributed first-key generation data in accordance with the third encryption algorithm to reproduce the second intermediate key;

means for encrypting the reproduced second intermediate key with the third block of the distributed first-key generation data in accordance with the fourth encryption algorithm to reproduce the first key.

wherein the descrambler further includes an authorization processor for processing the distributed first-key generation in order to enable the descrambler.

19. A descrambler according to claim 14 for descrambling an information signal scrambled by a said system, wherein the first-key generation data includes a quantity of data that must be processed by an authorization processor in the descrambler in order to enable the descrambler, and wherein said quantity of data exceeds the encryption capacity of a single operation of said first encryption algorithm; and in which system the first key is produced by encrypting a first block of the first-key generation data with the first-key prekey in accordance with the first encryption algorithm to produce a first intermediate key; processing a second block of the first-key generation data with the first intermediate key to produce a preencrypted second block of data; encrypting the preencrypted second block of data with a third block of the first-key generation data in accordance with a third encryption algorithm to produce an encrypted second block of data; processing the encrypted second block of data with the second block of data to produce a second intermediate key; processing a fourth block of the first-key generation data with the second intermediate key to produce a preencrypted fourth block of data; encrypting the preencrypted fourth block of data with a fifth block of the first-key generation data in accordance with a fourth encryption algorithm to produce an encrypted fourth block of data; and process-

ing the encrypted fourth block of data with the fourth block of data to produce the first key,

wherein the means in the descrambler for reproducing the first key comprise

means for encrypting the first block of the distributed first-key generation data with the reproduced first-key prekey in accordance with the first encryption algorithm to reproduce the first intermediate key;

means for processing the second block of the distributed first-key generation data with the reproduced first intermediate key to reproduce the preencrypted second block of data;

means for encrypting the reproduced preencrypted second block of data with the third block of the distributed first-key generation data in accordance with the third encryption algorithm to reproduce the encrypted second block of data;

means for processing the reproduced encrypted second block of data with the second block of data to reproduce a second intermediate key;

means for processing the fourth block of the distributed first-key generation data with the reproduced second intermediate key to reproduce the preencrypted fourth block of data;

means for encrypting the reproduced preencrypted fourth block of data with the fifth block of the distributed first-key generation data in accordance with the fourth encryption algorithm to reproduce the encrypted fourth block of data; and

means for processing the reproduced encrypted fourth block of data with the fourth block of data to reproduce the first key;

wherein the descrambler further includes an authorization processor for processing the distributed first-key generation data in order to enable the descrambler.

20. A descrambler according to claim **14** for descrambling an information signal scrambled by a said system in which the first-key generation data includes a sequence number associated with the second key,

wherein the means for providing the second key include means for processing the distributed sequence number to provide the second key.

21. A descrambler according to claim **20** for descrambling an information signal scrambled by a said system in which the key generation data further includes a key index used for accessing data processed to provide the second key in the descrambler,

wherein the means for providing the second key further include means for processing the distributed key index to provide the second key.

22. A descrambler according to claim **14** for descrambling an information signal scrambled by a said system in which the key generation data includes a key index used for accessing data processed to provide the second key in the descrambler,

wherein the means for providing the second key include means for processing the distributed key index to provide the second key.

23. A descrambler according to claim **14** for descrambling an information signal scrambled by a said system in which the first key is processed to produce the keystream by encrypting third key generation data with the first key in accordance with a third encryption algorithm to produce a third key; and the third key is processed to produce the keystream; and the third key generation data is also distributed,

wherein the means for processing the reproduced first key to reproduce the keystream, comprise

means for encrypting the distributed third key generation data with the reproduced first key in accordance with the third encryption algorithm to reproduce the third key; and

means for processing the reproduced third key to reproduce the keystream.

24. A descrambler according to claim **14** for descrambling an information signal scrambled by a said system in which first-key prekey generation data is encrypted with a first-key prekey prekey in accordance with a third encryption algorithm to produce the first-key prekey; the first-key prekey prekey is encrypted with the second key in accordance with a fourth encryption algorithm to produce an encrypted first-key prekey prekey; and the encrypted first-key prekey prekey, the first-key prekey generation data and a descrambler category identification number are also distributed, wherein the descrambler further comprises

means for decrypting the distributed encrypted first-key prekey prekey with the second key in accordance with the fourth encryption algorithm to reproduce the first-key prekey prekey;

means for encrypting the distributed first-key prekey generation data with the reproduced first-key prekey prekey in accordance with the third encryption algorithm to reproduce the first-key prekey; and

switching means responsive to the distributed descrambler category identification number for causing the first-key prekey that is used to encrypt the distributed first-key generation data to be reproduced by either (a) decrypting the distributed encrypted first-key prekey with the second key in accordance with the second algorithm or (b) decrypting the distributed encrypted first-key prekey prekey with the second key in accordance with the fourth algorithm to reproduce the first-key prekey prekey and encrypting the distributed first-key prekey generation data with the reproduced first-key prekey prekey in accordance with the third algorithm.

* * * * *